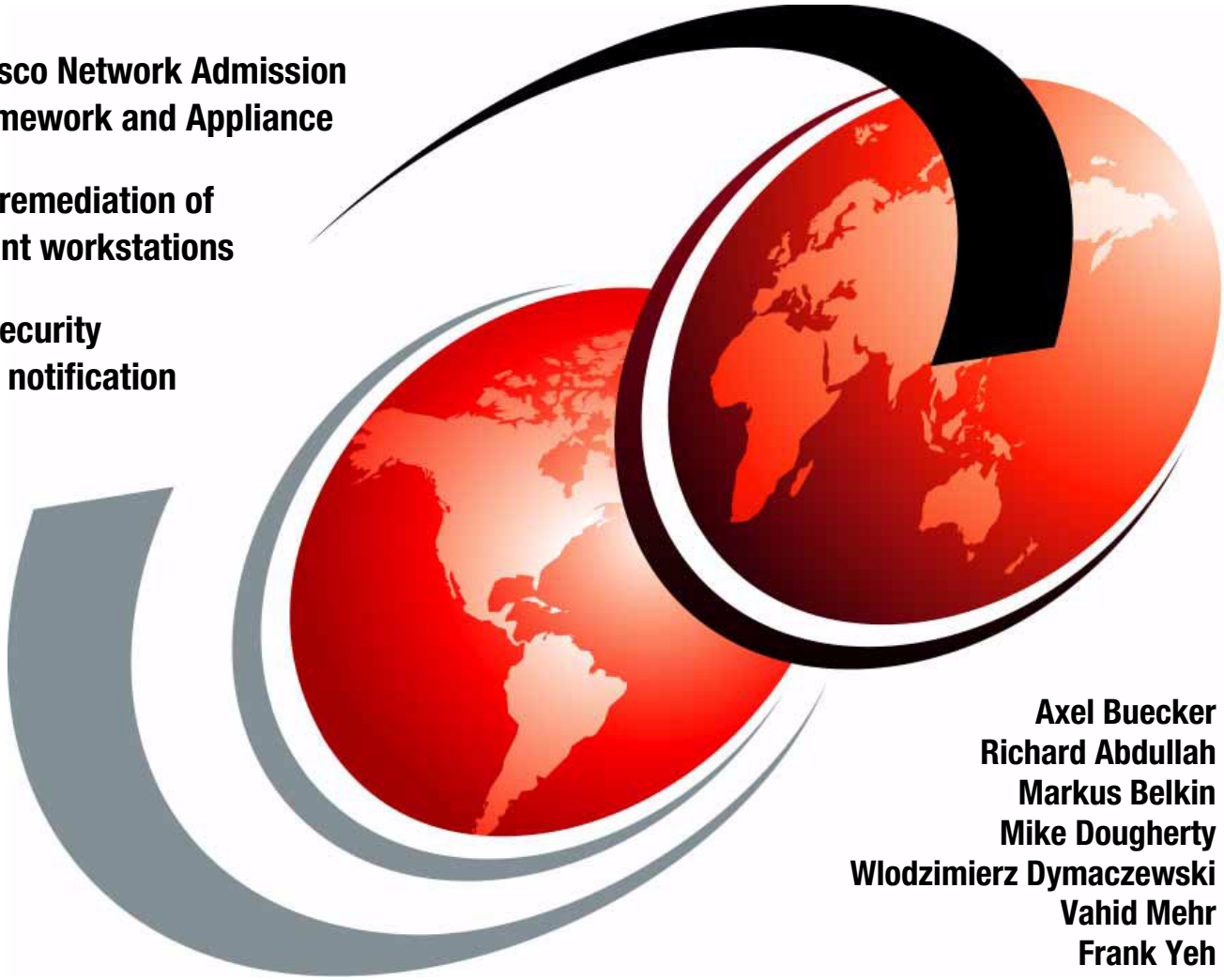
Tivoli software

IBM

Building a Network Access Control Solution

with IBM Tivoli and Cisco Systems

- Covering Cisco Network Admission Control Framework and Appliance
- Automated remediation of noncompliant workstations
- Advanced security compliance notification



Axel Buecker
Richard Abdullah
Markus Belkin
Mike Dougherty
Wlodzimierz Dymaczewski
Vahid Mehr
Frank Yeh

Redbooks

ibm.com/redbooks

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

International Technical Support Organization

Building a Network Access Control Solution with IBM Tivoli and Cisco Systems

January 2007

SG24-6678-01

Downloaded from www.Manualslib.com manuals search engine

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

Second Edition (January 2007)

This edition applies to Tivoli Security Compliance Manager V5.1, Tivoli Configuration Manager V4.2.3, and Cisco Secure ACS V4.0.

© Copyright International Business Machines Corporation 2005, 2007. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Downloaded from www.Manualslib.com manuals search engine

Contents

Notices vii
Trademarks viii

Preface ix
The team that wrote this redbook x
Become a published author xii
Comments welcome xiii

Summary of changes xv
January 2007, Second Edition xv

Part 1. Architecture and design 1

Chapter 1. Business context 3
1.1 The security compliance and remediation concept 4
1.2 Why we need this 5
1.3 Does this concept help our mobile users 7
1.4 Corporate security policy defined 8
1.5 Business driver for corporate security compliance 8
1.6 Achievable benefits for being compliant 9
1.7 Conclusion 10

Chapter 2. Architecting the solution 13
2.1 Solution architectures, design, and methodologies 14
2.1.1 Architecture overview 14
2.1.2 Architectural terminology 19
2.2 Definition of a Network Admission Control project 26
2.2.1 Phased rollout approach 26
2.3 Design process 28
2.3.1 Security compliance management business process 28
2.3.2 Security policy life cycle management 30
2.3.3 Solution objectives 32
2.3.4 Network design discussion 33
2.4 Implementation flow 35
2.5 Scalability and high availability 35
2.6 Conclusion 37

Chapter 3. Component structure 39
3.1 Logical components 40

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

3.1.1 Network Admission Control 41
3.1.2 Compliance 46
3.1.3 Remediation 51
3.2 Physical components 52
3.2.1 Network client 52
3.2.2 Network access infrastructure 54
3.2.3 IBM Integrated Security Solution for Cisco Networks servers 54
3.3 Solution data and communication flow 55
3.3.1 Secure communication 62
3.4 Component placement 63
3.4.1 Security zones 63
3.4.2 Policy enforcement points 67
3.5 Conclusion 74

Part 2. Customer environment 75

Chapter 4. Armando Banking Brothers Corporation 77
4.1 Company profile 78
4.2 Current IT architecture 79
4.2.1 Network infrastructure 79
4.2.2 IBM Integrated Security Solution for Cisco Networks lab 80
4.2.3 Application security infrastructure 85
4.2.4 Middleware and application infrastructure 86
4.3 Corporate business vision and objectives 87
4.3.1 Project layout and implementation phases 87
4.4 Conclusion 91

Chapter 5. Solution design 93
5.1 Business requirements 95
5.2 Functional requirements 96
5.2.1 Security compliance requirements 96
5.2.2 Network access control requirements 96
5.2.3 Remediation requirements 97
5.2.4 Solution functional requirements 97
5.3 Implementation architecture 101
5.3.1 Logical components 102
5.3.2 Physical components 116
5.4 Conclusion 123

Chapter 6. Compliance subsystem implementation 125
6.1 Tivoli Security Compliance Manager setup 126
6.1.1 Installation of DB2 database server 126
6.1.2 Installation of Tivoli Security Compliance Manager server 140
6.2 Configuration of the compliance policies 152

Downloaded from www.Manualslib.com manuals search engine

6.2.1 Posture collectors . . . 153
6.2.2 Policy collector . . . 154
6.2.3 Installation of posture collectors . . . 155
6.2.4 Customization of compliance policies . . . 161
6.2.5 Assigning the policy to the clients . . . 186
6.3 Deploying the client software . . . 189
6.3.1 Cisco Trust Agent . . . 190
6.3.2 IBM Tivoli Security Compliance Manager client . . . 199
6.4 Conclusion . . . 212

Chapter 7. Network enforcement subsystem implementation . . . 213
7.1 Configuring NAC Framework components . . . 214
7.1.1 Configuring the Cisco Secure ACS for NAC L2 802.1x . . . 214
7.1.2 Configuring the Cisco Secure ACS for NAC L2/L3 IP . . . 283
7.1.3 Deployment of the network infrastructure . . . 291
7.2 Configuring NAC Appliance components . . . 303
7.2.1 Installing CCA Agent . . . 304
7.2.2 Configuring a CCA OOB VG server . . . 306
7.2.3 Deployment of the network infrastructure . . . 352
7.3 Conclusion . . . 354

Chapter 8. Remediation subsystem implementation . . . 355
8.1 Automated remediation enablement . . . 357
8.2 Remediation server software setup . . . 358
8.2.1 Prerequisites . . . 358
8.2.2 Tivoli Configuration Manager . . . 359
8.2.3 Configuration of the remediation server . . . 385
8.2.4 Installation of the Software Package Utilities . . . 394
8.3 Creating remediation instructions for the users . . . 397
8.3.1 Locating HTML . . . 398
8.3.2 Variables and variable tags . . . 402
8.3.3 Debug attributes . . . 406
8.3.4 Creating HTML pages for ABBC policy . . . 409
8.4 Building the remediation workflows . . . 417
8.4.1 Modification of the remediation packages . . . 436
8.5 Conclusion . . . 437

Part 3. Appendixes . . . 439

Appendix A. Hints and tips . . . 441
Deployment overview . . . 442
Top-level sequence of events . . . 444
Security Compliance Manager and NAC compliance subsystem . . . 446
Cisco NAC sequence of events . . . 447

Downloaded from www.Manualslib.com manuals search engine

Fault isolation 448
Security Compliance Manager server and client 450
Communication port usage 451
Tools and tricks 451
Cisco NAC. 451
Tools and tricks for the client 453
NAC Appliance details 455
NAC Appliance integration 457
Conclusion 470

Appendix B. Network Admission Control 471
Executive summary 472
The benefit of NAC. 472
Dramatically improve network security. 473
NAC implementation options 474
The NAC Appliance. 475
NAC Framework solution 476
Investment protection 476
Planning, designing, and deploying an effective NAC solution 477
The next steps 478
NAC technology 478
NAC Appliance components 478
NAC Framework components 479

Appendix C. Additional material 481
Locating the Web material 481
Using the Web material 482
How to use the Web material 482

Related publications 483
IBM Redbooks 483
Other publications 483
Online resources 484
How to get IBM Redbooks 484
Help from IBM 485

Index 487

Downloaded from www.Manualslib.com manuals search engine

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ™	DB2 Universal Database™	Redbooks™
developerWorks®	DB2®	Tivoli®
ibm.com®	IBM®	WebSphere®
Access360®	NetView®	
AIX®	PartnerWorld®	

The following terms are trademarks of other companies:

Cisco, Cisco Systems, Cisco IOS, PIX, and Catalyst are trademarks of Cisco Systems, Inc. in the United States, other countries, or both.

Java, JVM, J2EE, Solaris, Sun, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Expression, Internet Explorer, Microsoft, Visual Basic, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Downloaded from www.Manualslib.com manuals search engine

Preface

In February of 2004, IBM® announced that it would be joining Cisco's *Network Admission Control* (NAC) program. In December of 2004, IBM released its first offering for the Cisco NAC program in the form of the IBM Tivoli® compliance and remediation solution. In June of 2005 the first edition of this IBM Redbook was published.

A number of subsequent updates from Cisco have changed the dynamics of the Network Access Control market, and have led to significant changes by IBM to our compliance and remediation solution. Foremost amongst these new developments are the release of Cisco's Phase 2 Network Admission Control architecture, the addition of the NAC Appliance to Cisco's offerings, and the addition of Tivoli Configuration Manager as a remediation component of the overall solution.

While this second edition addresses these changes, the fundamental concept and business value of the solution remain relatively constant and are preserved with minimal changes from the first edition. In contrast, the technical and implementation details have significantly changed and are of great interest to those who have read the first edition.

It is important to realize what is the compliance and remediation solution. It is not a one-size-fits-all product that will work out-of-the-box for customers. It is an integrated solution comprised of three products that are very powerful in their own right. As such, there is no individual product manual that can properly capture all of the techniques and practices that must be developed in order to properly deploy this solution.

A typical product manual is analogous to an automobile owner's manuals in that it tells you a wealth of information about your product but it does not tell you how to apply your product in practice, just as an automobile owner's manual does not teach you how to drive or how to navigate. This redbook serves as a high-level guide for designing and deploying the solution in various business scenarios. It teaches you how to *drive and navigate* the compliance and remediation solution.

Note that the IBM Integrated Security Solution for Cisco Networks, referenced numerous times in this book, is a portfolio of solutions that also includes Tivoli's identity management solution for Cisco network access. This book does not address the identity-based solution, so any references to the IBM Integrated Security Solution for Cisco Networks in this book actually refers to the compliance and remediation parts of the solution.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working for the International Technical Support Organization, Austin Center. The project was executed at the Cisco Headquarter in San Jose.

Figure 1 Top left to right: Frank, Axel, Vahid, and Mike
Bottom left to right: Vlodek, Markus, and Rich

Axel Buecker is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide in Software Security Architecture and Network Computing Technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 20 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Downloaded from www.Manualslib.com manuals search engine

Richard Abdullah is a Consulting Engineer with Cisco Systems Strategic Alliances. Prior to joining Cisco Systems in 2001, he worked in technical capacities within various service providers. He has spent 19 years in the IT industry focusing on networking and most recently on network security solutions. He holds a BSEE degree from the University of Michigan, Dearborn.

Markus Belkin is a Network Architect with IBM Australia. He has worked in the IT Industry for 10 years and works predominately with Cisco technologies. He specializes in routing and switching, security and optical technologies. He has an MCP, MCSE, CCNA, CCDA, CCNP, and CCDP and is currently working towards his Routing and Switching CCIE.

Mike Dougherty is a Consulting Engineer at Cisco Systems, Inc. in San Jose, California. He has worked in the industry for 16 years supporting Cisco networking equipment ranging from routers and switches to security and unified communication solutions. He obtained his CCIE in Routing and Switching in 1996 and is currently working on his CCIE in Security. Mike is a technical consultant working in Strategic Alliances under the business development umbrella at Cisco Systems, Inc.

Wlodzimierz Dymaczewski is an IBM Certified Senior IT Specialist with IBM Software Group in Poland. Before joining the Tivoli Technical Sales team in 2002 he worked for four years in IBM Global Services where he was a technical leader for several Tivoli deployment projects. He has almost 13 years of experience in systems management, recently specializing in security. He holds a degree in Computer Science from the Poznan Technical University, Poland. Vlodek is a Certified Deployment Professional for Security Compliance Manager 5.1 and Risk Manager 4.1 as well as for some Tivoli automation products (TEC, NetView®, and Monitoring).

Vahid Mehr is a Consulting Engineer with Cisco Systems Strategic Alliances working on joined architectural solutions with IBM. In his more than 13 years of experience with Cisco he has been in various customer consulting and alliance development roles. Prior to this, he was a Software Engineer working on Object Oriented programming. He has a BSEE from the University of Colorado and resides in San Ramon, California.

Frank Yeh is a member of the IBM Corporate Security Strategy Team who works in Costa Mesa, California. He has more than 25 years of computing experience in a variety of functions including Operations, Support, MIS, Development, Sales, and Business Development. Prior to joining IBM, Frank served as the Strategic Architect for Access360®, a pioneer in the Identity Management space that was acquired by IBM in October 2002. He holds a degree in Economics from the University of California, Los Angeles.

Downloaded from www.Manualslib.com manuals search engine

Thanks to the following people for their contributions to this project:

Cheryl Gera, Erica Wazewski, Lorinda Schwarz, Julie Czubik
International Technical Support Organization, Poughkeepsie Center

Wing Leung, Alex Rodriguez
IBM US

Tadeusz Treit, Bogusz Piotrowski, Anna Iskra
IBM Poland

Cindra Ford, Zary Stahl, Nick Chong, Prem Ananthakrishnan, Brendan O'Connell, Irene Sandler, Raju Srirajavatchavai, Alok Agrawal, Marcia Hanson
Cisco Systems Inc.

Thanks to following people for working on the first edition of this book:
Wlodzimierz Dymaczewski
Jeffery Paul
John Giammanco
Harish Rajagopal
Hideki Katagiri

Additional support: Tom Ballard, Sam Yang, Mike Garrison, Max Rodriguez, Don Cronin, Michael Steiner, Jeanette Fetzer, Sean Brain, Sean McDonald
IBM US

Phil Billin
IBM UK

Richard Abdullah, Mike Steinkoenig, Denise Helfrich, Laura Kuiper, Cindra Ford, Vahid Mehr
Cisco Systems, Inc.

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, IBM Business Partners, and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Downloaded from www.Manualslib.com manuals search engine

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-6678-01
for Building a Network Access Control Solution with IBM Tivoli and Cisco Systems
as created or updated on January 16, 2007.

January 2007, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- The Cisco Network Admission Control Appliance has been added to the network access control solution.
- The IBM Tivoli Configuration Manager has been added to the remediation solution. It replaces the IBM Tivoli Provisioning Manager product.

Changed information

- A new release of IBM Tivoli Security Compliance Manager is being used within the security compliance solution.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Part 1

Architecture and design

In this part we discuss the overall business context of the IBM Integrated Security Solution for Cisco Networks. We then describe how to technically architect the overall solution into an existing environment, and introduce the logical and physical components on both the IBM Tivoli and Cisco side.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

1

Business context

Information Technology (IT) security is a vital component of business success and is very important in e-business security and security for on demand services. As the Internet increasingly becomes an effective means to conduct business, the challenge of protecting IT infrastructures from intruders and malicious attacks increases as well. When an IT resource (server, workstation, printer, and so on) is connected to a network, it becomes a target for a persistent hacker. Corporate networks are constantly under attack by intruders seeking access for their personal gain. In a world where everyone relies on the Internet, it is not difficult for an intruder to find the tools on the Web to assist in breaking into an enterprise network. To overcome this immense threat faced by many organizations, a corporation must identify every user accessing its network and allow access only to authorized users who are identified and meet *corporate compliance* criteria.

Every time an intruder successfully breaks into a corporate network or infects computers with a virus or malicious code, it can cause damage that may result in *substantial financial loss* (loss of revenue) to the businesses involved. Enterprises must defend their IT infrastructure continuously and keep themselves protected from intruders. One infected server or workstation can potentially bring the whole corporate network to its knees if it does not comply with corporate security policies.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Personal computer workstations are used in the office, at home, or at a remote client location. Telecommuters must use mobile PC workstations to meet customer expectations and provide quicker response to queries, quotes, and information.

In this book, we introduce a new concept: a *comprehensive integrated security solution* jointly developed by IBM and Cisco Systems, trusted leaders in this arena for many years who have established enviable synergy in the industry. This solution is based on the IBM Enterprise Class Autonomic Computing Model and the Cisco Self-Defending Network. This new concept provides an integrated security model that can help an organization protect its reputation by enabling its network to self-defend. This also enables corporations to proactively secure IT infrastructure and protect from loss of productivity, loss of revenue, and the constant battle of escalation due to noncompliance. Every time an auditor finds an IT resource that is noncompliant, it costs the enterprise a lot of money to fix (reactive measure) and to regain compliance, which leads to loss of productivity. Security auditors can even shut down a mission-critical server or deny access to users if found to be vulnerable due to noncompliance.

The solution discussed in this book addresses corporations' security concerns by validating users against a centrally predefined policy before granting them access to the network. It also provides a path for an automated remediation process to fix noncompliant workstations quickly (improved productivity).

This solution can be deployed in stages by first targeting the most vulnerable user community, such as wireless local area network (WLAN) users or a branch office that is less secure, and then expanding the deployment enterprise-wide. This concept resolves the human-intensive process that is involved in fixing infected workstations that do not have antivirus software or the latest antivirus signature and so on. This concept further helps customers to act proactively in defending their network by denying access to unauthorized users.

1.1 The security compliance and remediation concept

IBM and Cisco are working together on this new concept that offers a solution to companies to defend their network. This solution is called the *IBM Integrated Security Solution for Cisco Networks*. The IBM Tivoli Security Compliance Manager (SCM) and Cisco Network Admission Control (NAC) integration in this solution can assist you in safeguarding your IT resources and enables security compliancy to users. The IBM Integrated Security Solution for Cisco Networks is a first of its kind in the industry that provides a full cycle self-defending and automated remediation mechanism to corporate networks. Both Security Compliance Manager and NAC are independent solutions. Combined, they complement each other and can provide the best *self-defending and compliance*

Downloaded from www.Manualslib.com manuals search engine

concept that can protect all networks in this era. This IBM and Cisco integration, depicted in an overview in Figure 1-1, is a true enabler for the on demand self-defending and security compliance strategy.

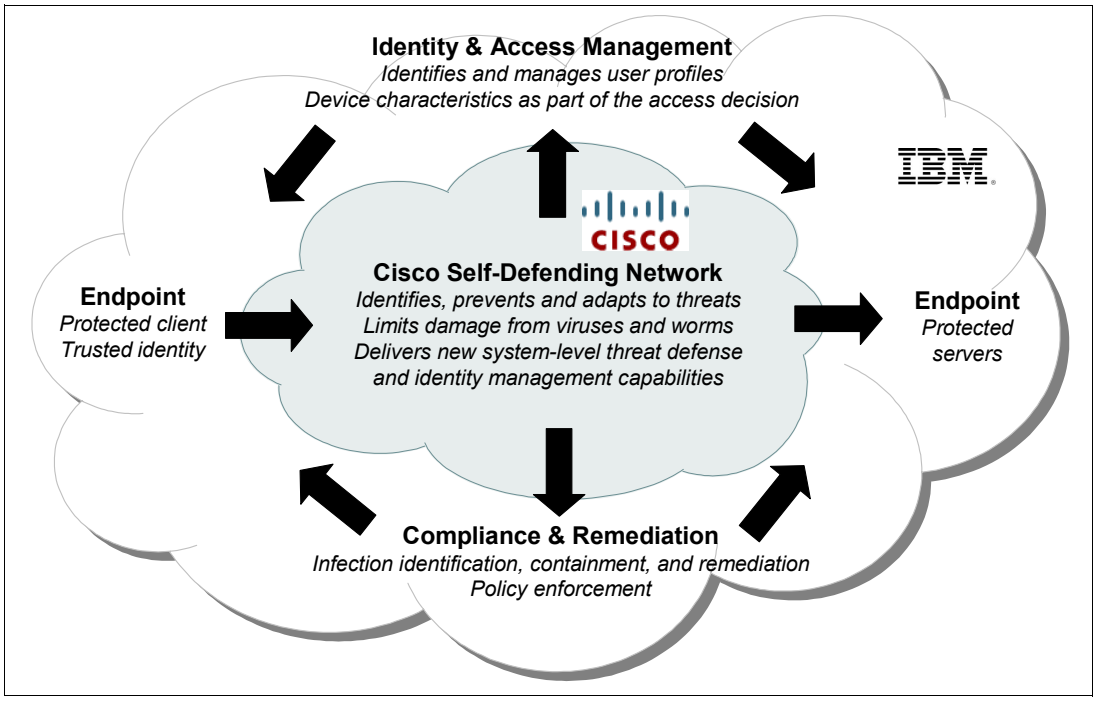


Figure 1-1 IBM and Cisco integration strategy

IBM Security Compliance Manager and Cisco Network Admission Control can help the corporate protect networks by identifying every client and denying access to the ones who are not identified. Further integrating Security Compliance Manager and NAC with the IBM Tivoli Identity Management suite can help corporations keep authorized users compliant with corporate security through central management of user profiles and policy enforcement.

1.2 Why we need this

Computer virus outbreaks create a dreadful situation for corporate CIOs, who must regard proactive protection against viruses as constant. The IBM Integrated Security Solution for Cisco Networks solution provides in-depth defense by ensuring that authorized users are kept compliant with corporate security policies and denying access to users who are noncompliant. With the integration of Tivoli Configuration Manager, the solution can provide a path to an *automated remediation* process to help noncompliant users get their workstations compliant again, which can result in *improved productivity*.

Downloaded from www.Manualslib.com manuals search engine

It has become mandatory for businesses to comply with regulatory guidelines such as the *Gramm-Leach-Bliley Act (GLBA;* also known as the *Financial Services Modernization Act*), *Sarbanes-Oxley Act (SOX),* and *Health Insurance Portability and Accountability Act (HIPAA)*. More guidelines may emerge over time.

The Gramm-Leach-Bliley Act has provisions to protect consumer information held by financial institutions. This act provides the authority for federal agencies to enforce and administer the *Financial Privacy Rule* and the *Safeguards Rule*.

Any company with stock that is publicly traded in the United States must comply with the Sarbanes-Oxley Act, regardless of whether the company's headquarters is located in the U.S. This compliancy requirement was enacted to protect individual investors, and corporations are required by law to provide truthful financial statements. All public financial statements released by corporations are subjected to intense scrutiny by regulatory authorities. Hence these legislations mandate every corporation to maintain the integrity of its own data and provide the same level of protection to the data it cares for.

Note: More information about the Gramm-Leach-Bliley Act (GLBA) can be found at:

`http://banking.senate.gov/conf/`

More information about the Sarbanes-Oxley Act (SOX) can be found at:

`http://www.sarbanes-oxley.com`

More information about the Health Insurance Portability and Accountability Act (HIPAA) can be found at:

`http://www.cms.hhs.gov/hipaa`

These laws are applicable for organizations in the United States of America. Similar regulations may be enforced by government regulators of other countries. Customers should consult their relevant government regulatory bodies to learn more about the applicable laws in their respective countries.

Downloaded from www.Manualslib.com manuals search engine

Note: Customers are responsible for ensuring their own compliance with various laws such as the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act. It is the customer's sole responsibility to obtain the advice of competent legal counsel regarding the identification and interpretation of any relevant laws that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal, accounting, or auditing advice, or represent or warrant that its products or services ensure that the customer is in compliance with any law.

The IBM Integrated Security Solution for Cisco Networks checks every client's workstation when it attempts to connect to the corporate local area network (LAN) using predefined policies. For example, it can examine whether the workstation has the latest antivirus signature installed, whether a desktop firewall is running, whether the password length is correct, and so on. When a noncompliant client is detected, the IBM Integrated Security Solution for Cisco Networks quarantines the client by denying access to the corporate LAN and directing that workstation to either automatically download the latest antivirus signature or provide information why the workstation is noncompliant. This provides an opportunity for the user to either manually download the required updates from the remediation LAN or choose a path to automatically remediate using IBM Tivoli Configuration Manager.

1.3 Does this concept help our mobile users

The IBM Integrated Security Solution for Cisco Networks by default denies access to the corporate LAN for all noncompliant users and keeps them at bay. Enforcing this policy requires every telecommuter's computer to be compliant before it is granted access to the corporate LAN.

Corporations must allow external partners and contractors to have access to limited IT resources as well. Most businesses are looking for ways to remotely connect to their corporate LAN using a secure virtual private network (VPN) connection from outside their office premises. The IBM Integrated Security Solution for Cisco Networks can be configured to allow only partners to connect to the Internet by using a policy that provides appropriate access to the partners' workstations that do not have particular client software installed on their computers. This can be considered a winning situation for both parties involved, as it provides a network access method without additional infrastructure and yet assures protection from non-authorized users.

Downloaded from www.Manualslib.com manuals search engine

Standard reports that can be generated from the IBM Integrated Security Solution for Cisco Networks can be valuable to corporate auditors. These can be used as artifacts, thereby reducing the effort in checking individual users. Automated processes can also provide consistency in checking a particular policy that may be required at certain circumstances. For example, when a new vulnerability is being publicized a policy can be created and deployed quickly to direct users to update their workstation and regain compliancy by downloading and installing a fix using the appropriate remediation process.

1.4 Corporate security policy defined

A corporate security policy should protect the company's valuable assets and meet legal obligations. Intellectual properties must not be shared without explicit written authorization. As we do business with customers, we are required by law to maintain the confidentiality of the information, privacy of the individual, and so on. Companies must adhere to government regulations that ensure that businesses are run legally and ethically without jeopardizing the integrity of the enterprise. This is fundamental to maintain a trusted relationship between organizations and customers. Many businesses have outsourced their IT management to third-party companies; now it is the responsibility of that company to maintain the data confidentiality and integrity.

Most large corporations have employee guidelines that define how to protect company assets and conduct business with customers. Each employee is solely responsible for their actions and has to perform business within the given framework or guidelines set by the company.

To maintain trust between organizations, security is everyone's concern without any exception. Every employee must be empowered to challenge untrusted entities, such as unauthorized access to information. Hackers use all abilities and means to access protected data. Physical security alone does not protect data, as information is available in many shapes and forms. It is of utmost importance for every employee of an organization to be conscious of corporate security policies and to adhere to them without exception.

1.5 Business driver for corporate security compliance

Corporations are required to enforce compliance to their policies to maintain a secure network and allow access only to authorized users, employees, and external partners. Best practices include:

- Protect the corporate network from malicious attackers.
- Keep authorized users compliant with corporate security policy.

Downloaded from www.Manualslib.com manuals search engine

- Enable an automated remediation process that eases the process of regaining compliancy for all authorized users on the corporate network.
- Provide partners and visitors access to the Internet but not the corporate intranet.

1.6 Achievable benefits for being compliant

How do organizations benefit from compliance with corporate security policies?

Corporate security policies and controls are established to enforce consistent rules that centrally secure access to IT resources across the organization. This also provides consistency in compliance with general business rules. Enforcing and maintaining strong passwords, for example, can make it more difficult for malicious users to access protected data.

Corporate auditors check for consistency in compliancy to corporate policies and look for deviations by individual users. Auditors are always looking for artifacts to prove that users are compliant. These can be used when the enterprise is being legally challenged by government regulators.

The following list spells out some tangible benefits to the organization:

- Increased accuracy of security compliance reporting
- Reduced effort and costs in data collection and report generation
- Timeliness of report generation and artifacts as required during security audits
- A consistent approach to security compliance reporting across geographically dispersed organizations

Downloaded from www.Manualslib.com manuals search engine

Figure 1-2 depicts the relevant tasks in a life-cycle overview for endpoint protection. All of the topics discussed in this chapter are represented at some point in this life cycle.

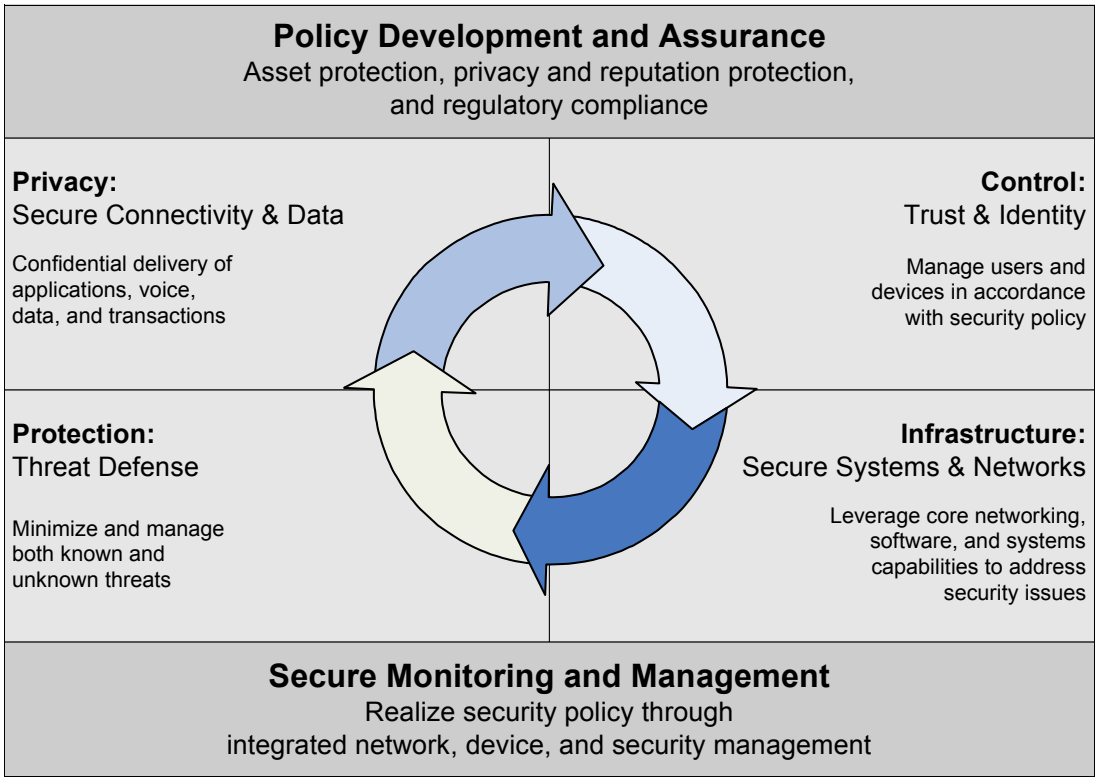

Policy Development and Assurance
Asset protection, privacy and reputation protection, and regulatory compliance
Privacy:
Secure Connectivity & Data
Confidential delivery of applications, voice, data, and transactions
Control:
Trust & Identity
Manage users and devices in accordance with security policy
Protection:
Threat Defense
Minimize and manage both known and unknown threats
Infrastructure:
Secure Systems & Networks
Leverage core networking, software, and systems capabilities to address security issues
Secure Monitoring and Management
Realize security policy through integrated network, device, and security management

Figure 1-2 Integrated endpoint protection

When an organization is responsible for maintaining and protecting customer data, it must create measures to ensure policy compliance by all involved systems on an automated and regular basis. Failure to meet this objective has resulted in significant exposure and many lawsuits have been lost. It is better to seem security-paranoid than to be ignorant.

More information about security compliance can be found in the IBM Redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450.

1.7 Conclusion

Organizations are constantly looking to maintain compliance status with their corporate security policy for both inter-company and intra-company interactions. Production losses and inefficiencies, and therefore substantial financial losses, have resulted from noncompliance. Laws and government regulations such as

Downloaded from www.Manualslib.com manuals search engine

those mentioned in 1.2, “Why we need this” on page 5, mandate every organization to comply with regulatory acts. Keys to greater productivity include identifying authorized users and providing them easier access to network and system resources while keeping them compliant.

The IBM Integrated Security Solution for Cisco Networks delivers corporate compliance at a reduced cost. The IBM Integrated Security Solution for Cisco Networks enables organizations to identify users, monitor their compliance, offer them an easy and centralized remediation capability in case of noncompliance, and easily route them into appropriate network zones based on their credentials.

IBM and Cisco have recognized inter-company and intra-company security compliance problems. This approach enables corporations to implement a *simplified, compliance-based full life-cycle Network Admission Control and remediation solution* that can result in greater productivity, consistency, and ease of user administration. It also enables the corporate auditors and administrators to have powerful controls in place for partners and contractors.

It is of utmost importance for every employee in an organization to be conscious of and in adherence with corporate security policies to provide end-to-end security across the gamut of IT services. Organizations must provide security education to all employees and continuously update on a regular basis; every employee from the CEO on down must comply. Security is the responsibility of *every employee,* not just the holder of the security job title.

In the next chapter we introduce the architecture and design methodologies for the IBM Integrated Security Solution using Cisco Networks.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

2

Architecting the solution

In this chapter we discuss the solution architecture of the IBM Integrated Security Solution for Cisco Networks with its compliance-based Network Admission Control system. We provide an overview of the key modules and their relationship, and describe an approach for introducing this additional security layer into the enterprise IT environment.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

2.1 Solution architectures, design, and methodologies

Our objective for this chapter is not to discuss any general approach for architecting a security solution; however, we follow the IBM Method for Architecting Secure Solutions (MASS), which is closely aligned with the Common Criteria objectives. IBM MASS uses a systematic approach for defining, modeling, and documenting security functions within a structured design process in order to facilitate greater trust in the operation of resulting IT solutions. More information about MASS may be found in the IBM Redbook *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

2.1.1 Architecture overview

The IBM Integrated Security Solution for Cisco Networks involves several products and components from IBM and Cisco Systems. In this section, we present an overview of the solution and define some of the terms used in subsequent sections and chapters.

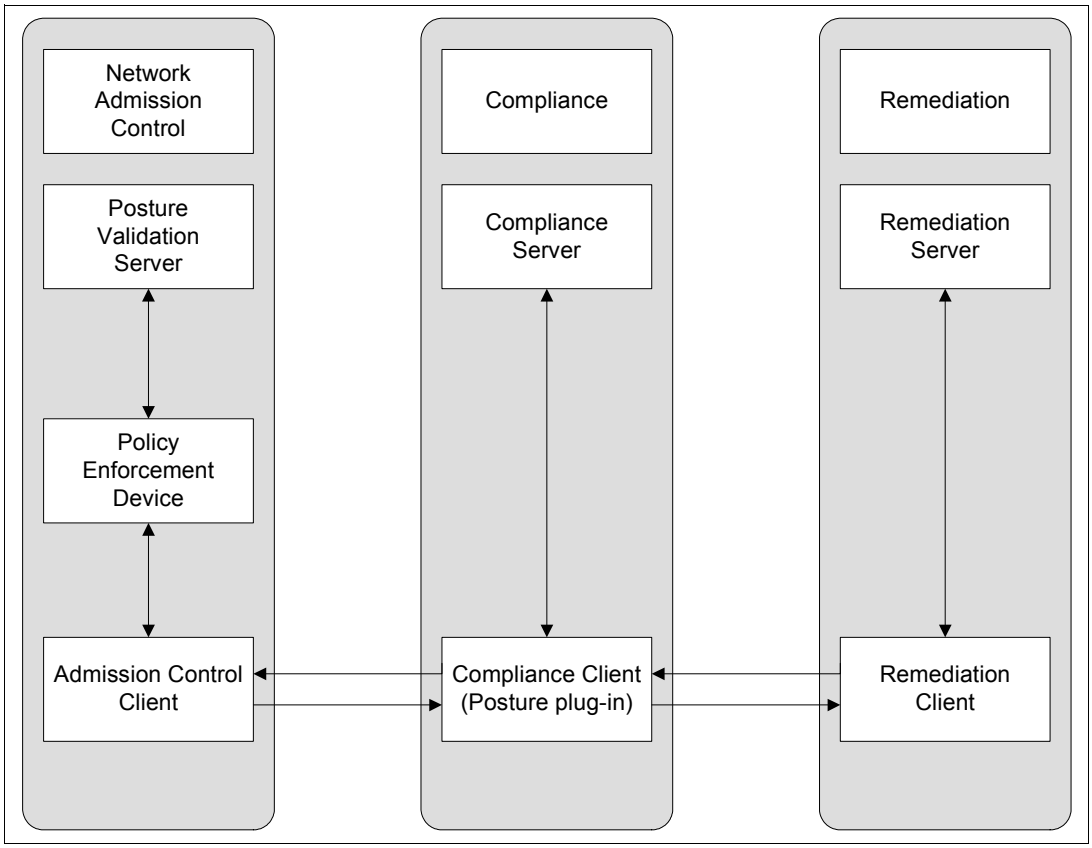


Figure 2-1 IBM Integrated Security Solution for Cisco Network components overview

Downloaded from www.Manualslib.com manuals search engine

In general, the IBM Integrated Security Solution for Cisco Networks consists of three subsystems or logical components, as shown in Figure 2-1 on page 14:

- Network Admission Control (NAC) subsystem based on Cisco technology
- Compliance subsystem based on IBM Tivoli Security Compliance Manager (SCM)
- Remediation subsystem based on IBM Tivoli Configuration Manager

Figure 2-2 depicts all involved subsystems and components in a physical network representation. It shows the involved stationary and portable clients, the different network segregations, the server components, and the required networking equipment.

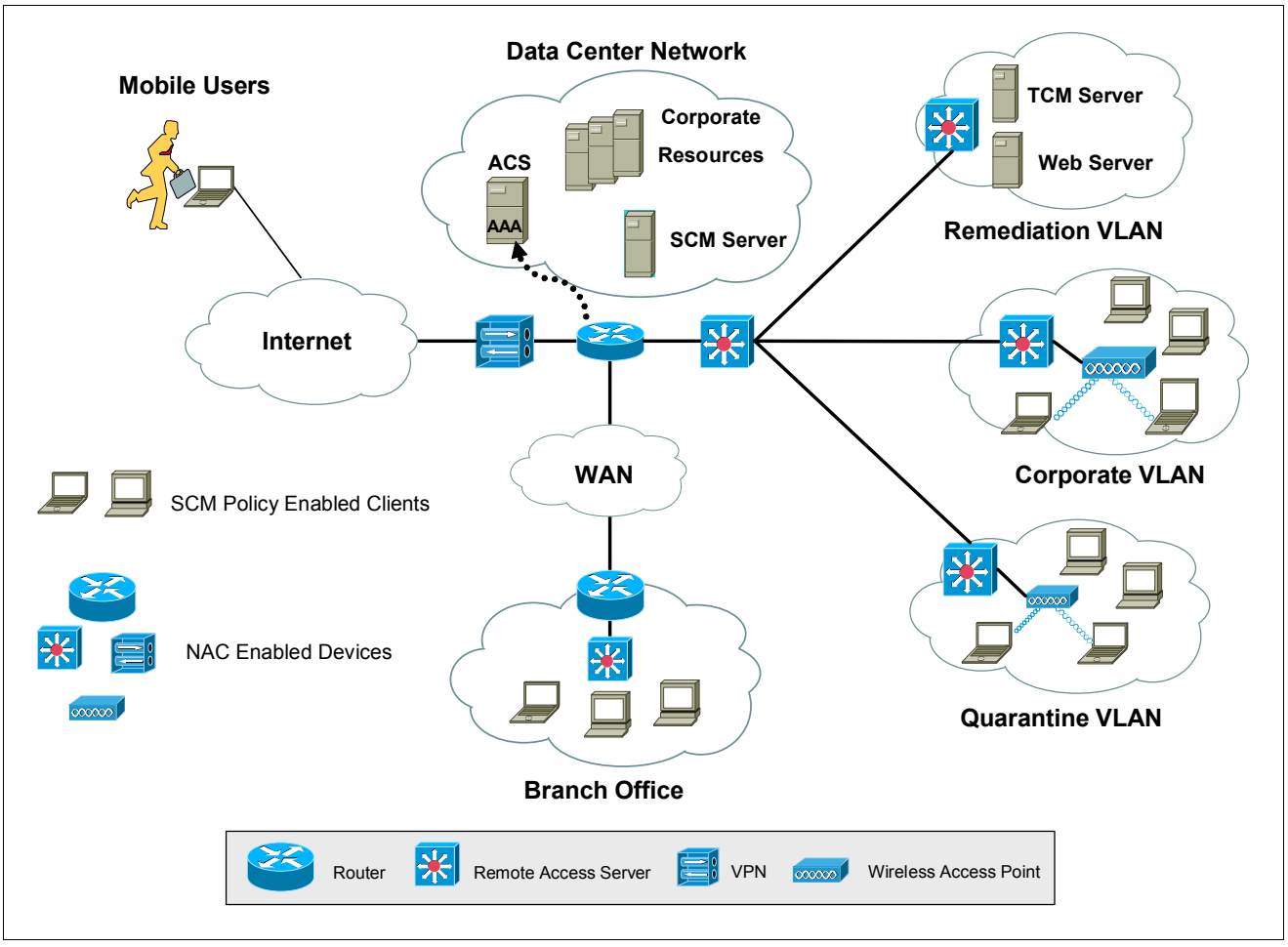


Figure 2-2 IBM and Cisco architecture overview

Network Admission Control

Network Admission Control (NAC) is a Cisco-sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all

Downloaded from www.Manualslib.com manuals search engine

devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with an established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them only restricted access to computing resources.

NAC is part of the *Cisco Self-Defending Network*, an initiative to increase network intelligence in order to enable the network to automatically identify, prevent, and adapt to security threats.

Network Admission Control offers the following benefits:

- *Comprehensive span of control* – All of the access methods that hosts use to connect to the network are covered, including campus switching, wireless access, router WAN links, IP Security (IPSec) remote access, and dialup.
- *Extension of existing technologies and standards* – NAC extends the use of existing communications protocols and security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services.
- *Extension of existing network and security software investments* – NAC combines existing investments in network infrastructure and security technology to provide a secure admission-control solution.

Network Admission Control is a strategic program in which Cisco shares technology features with approved program participants. Participants design and sell third-party client and server applications that incorporate these features that are compatible with the Network Admission Control (NAC) infrastructure.

Network Admission Control can operate at Layer 3 or Layer 2. In Cisco terms, *Layer 3 NAC* uses EAP transported on UDP packets and is called EAPoverUDP, or EOU. In *Layer 2 NAC* the Extensible Authentication Protocol (EAP) is transported on 802.1x frames and is called EAPoverLAN or EAPOL.

Downloaded from www.Manualslib.com manuals search engine

Note: With the availability of Cisco's Network Admission Control Appliance (NAC Appliance) offering, the Network Admission Control subsystem can be delivered by NAC Framework or NAC Appliance. While the interfaces between these two offerings vary, the Tivoli Security Compliance Manager and Tivoli Configuration Manager subsystems are designed to work with either version of Cisco's NAC offerings. A minor difference exists in the interface between Tivoli Security Compliance Manager and the selected Network Admission Control offering, but all of the policies and remediation objects built for Tivoli Security Compliance Manager and Tivoli Configuration Manager can be used interchangeably with either Cisco offering.

Customers have to choose between a NAC Framework and NAC Appliance implementation because applications that are compatible with a NAC Framework do not work with an NAC Appliance, as the interfaces are currently dissimilar. It is Cisco's stated intention to make NAC Framework and NAC Appliance solutions compatible, but at the current time, this is not the case.

In most cases, customers who run homogenous Cisco networks and have long-range NAC plans will be able to start with NAC Framework and deploy in phases. For customers with heterogeneous networks containing non-Cisco equipment or customers who wish to start with a smaller entry price and deployment footprint while still retaining the option to migrate to a full NAC Framework solution, NAC Appliance is the better choice.

For the purposes of this book, the majority of the content is targeted at NAC Framework solutions.

Security Compliance Manager

IBM Tivoli Security Compliance Manager performs the functions of managing security compliance policies and monitoring compliance of clients to these policies. It plays a vital role in deploying predefined policies and providing a repository for reporting that can help corporate auditors. The Security Compliance Manager server has a built-in reporting engine that can be used to produce standard reports as required by security officers. It can also utilize external report generators such as IBM DB2® Alphablox or Crystal Reports for ad hoc reporting.

The relationship between the Security Compliance Manager server and client is more accurately described as an agent/manager model than a client/server architecture. The Security Compliance Manager client acts as an agent collecting data from the client subsystem on a predefined schedule or at the request of the Security Compliance Manager server and sends the requested data back to the server. The Security Compliance Manager server acts as a manager issuing requests to clients and receiving data collections from the client.

Downloaded from www.Manualslib.com manuals search engine

Port details and communication flows between Security Compliance Manager server and client can be found in “Security Compliance Manager server and client” on page 450.

Details of the activities performed by server and client include:

- Security Compliance Manager server
  - Provides an interface for defining complex policies that specify conditions that should exist on a client.
  - Manages *when* the security compliance data is collected and which clients collect what kind of data using the data collection components.
  - Determines *what* security compliance data is collected, and how to interpret the data using the compliance management components.
  - Stores the security compliance data received from the clients in a central database and provides the available data to users through the administration console and administration commands.
  - Provides security violation details as a basis for the compliance report components.
- Security Compliance Manager client
  - Collects information about its environment required to assess compliance with the security policy at a predefined schedule. Using different *collectors*, this data is sent back to the Security Compliance Manager server. With new *posture collectors* introduced with Security Compliance Manager Fix Pack 2, the data is stored locally in a posture cache.
  - If enabled for NAC, the client performs a local compliance assessment using the security policy based on the data from the posture cache. It then provides the posture assessment data to the Cisco Trust Agent via posture plug-in for further processing.
  - Receives the network admission decision from either the Cisco Secure Access Control Server (ACS) via Cisco Trust Agent (in case of using the NAC Framework solution) or the Clean Access Server (CAS) via the Clean Access Agent (in case of using the NAC Appliance solution) and presents current status information using a GUI. It displays the compliance status and posture data, and enables re-initiating the compliance scanning process.
  - On user request, it can initiate an automated remediation process.

More information about Tivoli Security Compliance Manager can be found in the IBM Redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450.

Downloaded from www.Manualslib.com manuals search engine

Tivoli Configuration Manager

IBM Tivoli Configuration Manager automates the manual provisioning and deployment process.

Tivoli Configuration Manager provides an automated software and patch distribution solution that can also run pre-built scripts on a client, essentially enabling the Tivoli Configuration Manager solution to install any conceivable software product on a client as well as change a client's local settings and state.

This functionality is used to provide the noncompliant workstation with the correct software and settings using reusable remediation objects.

These remediation objects can be triggered automatically after a client has been tagged noncompliant by the Security Compliance Manager client policy evaluation process. This can help an individual client regain its compliance status and access to the production network without manual interaction and within an acceptable time frame.

A Tivoli Configuration Manager administrator must pre-define all of the objects necessary to remediate a noncompliant condition on a client. More information about Tivoli Configuration Manager can be found in the *Deployment Guide Series: IBM Tivoli Configuration Manager*, SG24-6454.

More details of each subsystem and its logical components can be found in Chapter 3, "Component structure" on page 39.

2.1.2 Architectural terminology

In this section we provide a brief introduction of the terms related to the solution described in this book, as illustrated in Figure 2-1 on page 14.

Security policy

A *security policy,* as implemented in Security Compliance Manager, is a collection of compliance objects or queries. A security policy defines what data has to be collected on the client (collectors and parameters) and the default schedule for gathering this data. Security policies can be applied to one or more client groups. The security policy uses a version attribute, which is required for the IBM Integrated Security Solution for Cisco Networks. Read more about these attributes in "Establishing the policy collector parameters" on page 104.

Compliance query

A *compliance query*, or *compliance object*, is a single check defined to verify one particular aspect of the enterprise security policy. Security Compliance Manager compliance objects are SQL queries extracting data from one or more collector

Downloaded from www.Manualslib.com manuals search engine

tables that contain data gathered by the collectors. In a generic Security Compliance Manager deployment, the compliance queries are evaluated on the server, but with NAC-enabled clients using new posture collectors they can also be evaluated on the client. A compliance query is written to return a list of policy violations.

The results of the compliance queries associated with a particular policy can be used on the Security Compliance Manager server to provide a current picture, or *snapshot*, of the level of compliance for all clients in a client group. The results of the compliance queries evaluated locally on the client are passed as a posture status. They define the client's compliance status.

Compliance User Interface

When a client is found to be out of compliance, the Tivoli Security Compliance Manager Client opens a window that notifies the user of the violation and provides a means to invoke the remediation process. This user interface includes a functional Web browser that supports customized HTML content that can assist the user in remediating. In addition, if an automated remediation handler is installed, a button to start automated remediation is presented to the user.

Remediation handler

A *remediation handler* performs the functions of communicating with the remediation server to download remediation content, installing downloaded content and providing respective notification to the user.

Network Admission Control process

The following are the conceptual steps of the Network Admission Control process. Figure 2-3 on page 21 displays the result of what happens to compliant, noncompliant, and clientless devices.

- A user tries to connect (remotely or locally) to the corporate network.
- A Network Access Device (NAD) challenges the client for compliance posture information.
- The Security Compliance Manager policy-enabled client communicates with the NAC system.
- The NAC system *validates* the client's health (posture) based on predefined rules.
- The NAC system either admits the client to the network if it complies with all of the policies or quarantines the client, allowing access only to a remediation network if the client is not complying with the policies.

Downloaded from www.Manualslib.com manuals search engine

- If the client is not Security Compliance Manager policy–enabled, it is *denied* access to the corporate network and may be allowed only *restricted access* to the Internet or may be *denied access* to all networks.
- When a client is quarantined, the user is given a choice to either *remediate* manually using the provided instructions or to use an *automated remediation* process by clicking a button on the pop-up window (if the Tivoli Configuration Manager infrastructure exists).

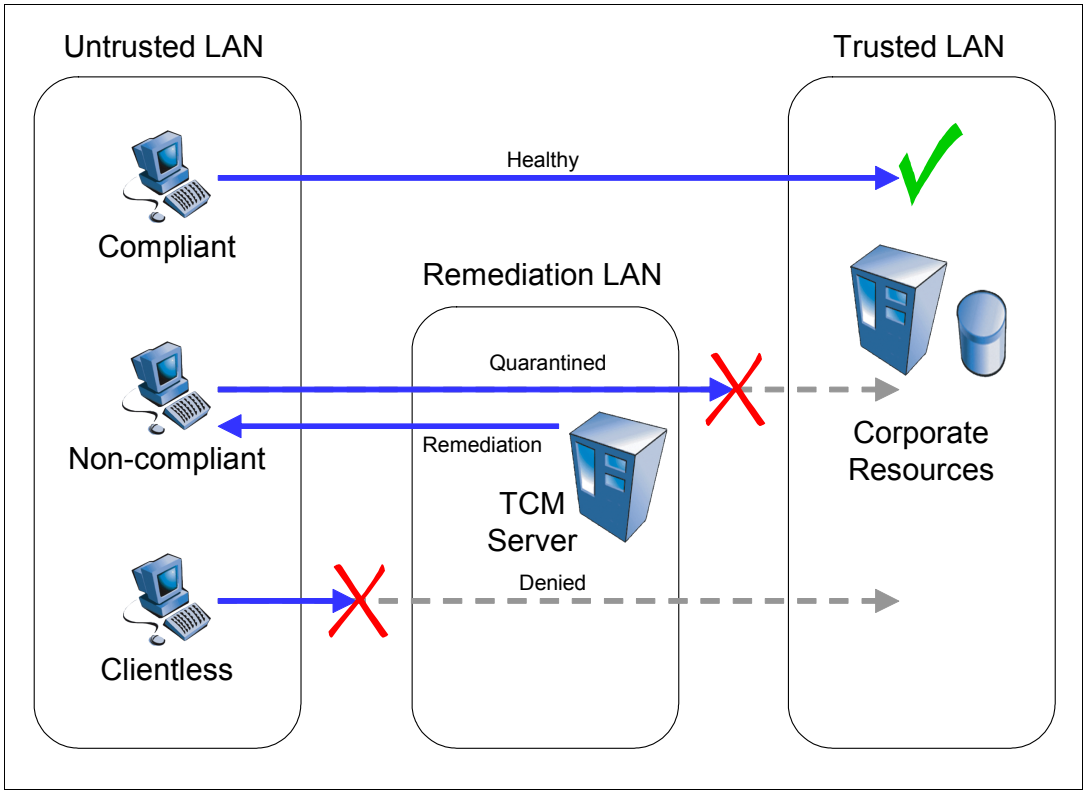


Figure 2-3 Basic overview of NAC functionality

In general, any admission control solution can base the admission decision on a number of factors. Authentication decisions are identity-based and the admission decisions are based on who is attempting access. Posture decisions are integrity-based and depend on the integrity of the device being used for access.

Posture-based NAC is designed to protect the network from threats introduced by noncompliant workstations. Workstation-related information is presented to the authorization server. It describes the current state of the hardware, operating system, and installed applications (for example, the list of patches installed, version of installed antivirus or personal firewall software, version of virus definition file, the date of the last full scan). With Layer 3 NAC, it is not straightforward to tie the identity-based and posture-based admission decisions together. Since they operate in two different time frames with regard to network

Downloaded from www.Manualslib.com manuals search engine

access, this is an acceptable solution. Users are authenticated and placed into a default network based on their identity. It is not until the user attempted access across a NAC-enabled router that the integrity check was performed.

With Layer 2 NAC, identity enforcement via 802.1x delivers access control by checking authorization of the user to connect to the network. The identity can be verified based on different means, such as user name/password or PKI public certificates, but more importantly, it allows both identity and posture to be validated before network access is granted. This allows users to be assigned into specific networks based on their identity and assigned groups with posture-based checking, providing an additional way to control a user's traffic.

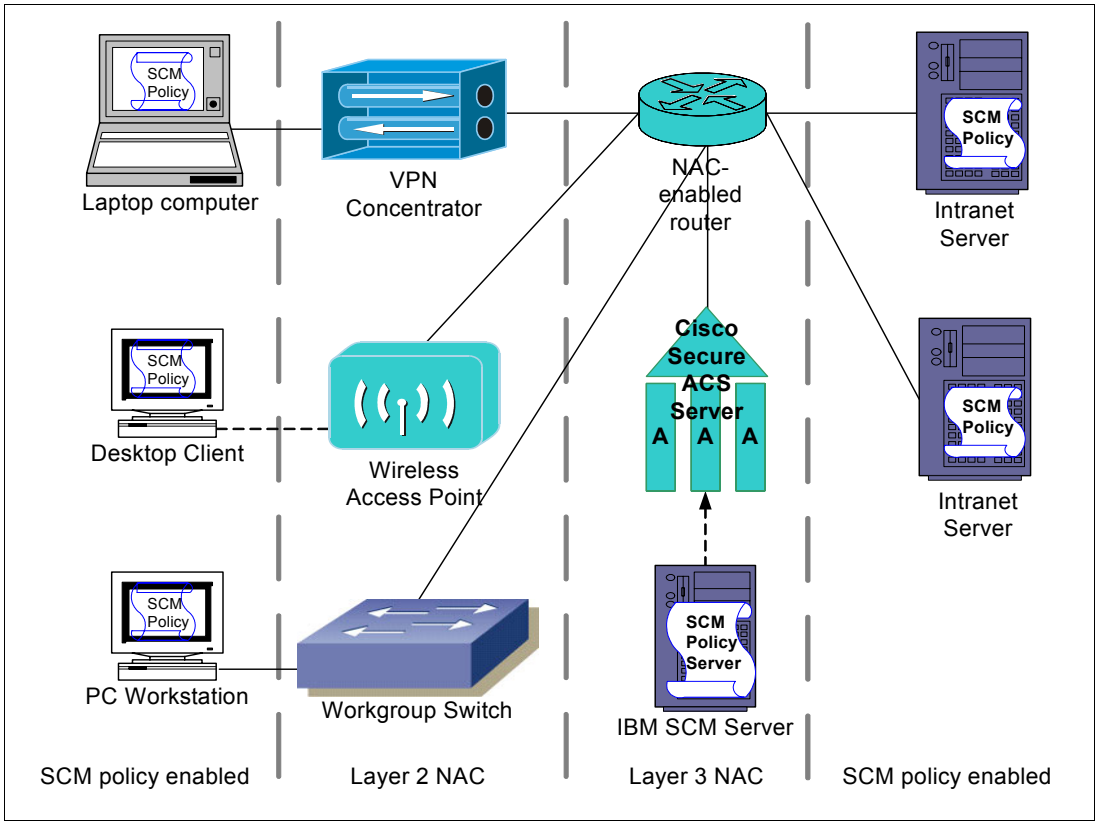


Figure 2-4 Layer 3 and Layer 2 NAC overview

Cisco NAC and IEEE 802.1x

An interesting terminology question to ask is: *How does this solution relate to the IEEE 802.1x protocol?* In this section we explain the basic difference and how these two solutions can complement each other.

IEEE 802.1x is an identity-based network authentication protocol used at Layer 2 level to allow or disallow a specific user to connect to the network based on user or machine credentials.

Downloaded from www.Manualslib.com manuals search engine

The IEEE 802.1x standard addresses the need to authenticate the user or client trying to connect to the particular network. Point-to-Point Protocol (PPP) can be used in a basic dial-up scenario, but it limits the authentication process to checking only user and password matching. The Extensible Authentication Protocol (EAP) was designed to provide transport for other authentication methods. EAP extends PPP as a framework for several different authentication methods, such as challenge-response tokens and PKI certificates.

IEEE 802.1X introduces three terms:

Supplicant	The user or device that wants to be authenticated and connect to the network.
Authenticator	The device responsible for mediation between client and authentication server. Typically this is a RAS server for EAP-over-PPP, or a wireless access point or switch for EAP-over-LAN.
Authentication server	The server performing authentication, typically a RADIUS server.

IEEE 802.1x was introduced to enable users to use EAP in a consistent way, with either dial-up or LAN connection. It defines the way an EAP message is packaged in an Ethernet frame so there is no need for PPP-over-LAN overhead.

On the other hand, Cisco NAC is a posture-based Network Admission Control solution that enables control of who connects to the network and whether the client workstation is *healthy* and complies with all *required security policies*.

The Cisco Layer 3 NAC solution implements proprietary extensions to EAP and uses User Datagram Protocol (UDP) as the transport for EAP (EAP-over-UDP, or EOU). In Cisco's Layer 2 NAC offerings, EAP is transported over 802.1x.

Using Cisco terminology

The Cisco Trust Agent performs the role of the supplicant. It provides the authenticator, which is a NAC-enabled Cisco device, with the client's posture statement. The communication is performed using the EAP-over-UDP or EAP-over-802.1X protocol. On the network device, the EAP header is repackaged into RADIUS and sent to the Cisco Secure ACS server (performing the role of an authentication server).

The main difference between IEEE 802.1x and the Cisco implementation lies in the authentication process:

- With generic IEEE 802.1x, the EAP header carries only identity information, and authentication is performed using credentials provided by the supplicant.

Downloaded from www.Manualslib.com manuals search engine

- In the Cisco NAC solution, the EAP header is extended with posture data and the admission process is based on policies governing the network admission decision. Those policies consider all of the attributes provided by the posture agent (Cisco Trust Agent) to determine the client's health and security compliance status.
- In the generic 802.1x, the identity credential is used for authentication.
- In the Cisco NAC solution, the posture credential of the client device is used for authentication.

IEEE 802.1x and NAC can be combined easily to provide a stepped-up level of security in corporate networks. The selected authentication and network admission protocols will determine which client software or supplicants are loaded on the client.

Note: In this section we used the term *authentication* to discuss the differences and similarities between IEEE 802.1x and the Cisco NAC process.

Regarding 802.1x, we can accurately speak of authentication because we are considering individuals providing credentials to gain access to protected resources. In the Cisco NAC process we examine a posture status of a client machine in order to grant general network access — a process not usually considered an authentication.

Posture agent

The *posture agent* is a software agent residing on the client capable of communicating with the NAC-enabled network device before the client is granted network access. It aggregates security posture information from the NAC-compliant applications running on the network client and sends it to the posture verification server. In the present solution, the role of the posture agent is performed by Cisco Trust Agent. Third-party applications including the IBM Tivoli Security Compliance Manager client register with the posture agent using a plug-in. More information can be found in 3.2.1, "Network client" on page 52.

Network identity provisioning

With the posture-based Network Admission Control, the client requires a set of software components to be able to connect to the network. It is feasible to assign different security policies to the different groups of clients and check for compliance with complex rules concerning all of the clients' attributes. However, all clients running the same version of an operating system, for example, typically are unified in terms of which security policy applies for these clients. Looking at the generic design, the NAC solution makes no differentiation between who the clients belong to or who is actually trying to connect to the network.

Downloaded from www.Manualslib.com manuals search engine

This requirement can be fulfilled by providing each user with a unique identity and verifying it even before the posture condition of a client is checked. This process was standarized with the IEEE 802.1x protocol, and IBM provides the solution to facilitate it. IBM Tivoli Identity Manager delivers a flexible provisioning engine to create and manage user accounts on the Secure Access Control Server. For more information, contact your IBM representative.

Remediation process

The *remediation process*, either HTML-assisted or automated, is an integral part of the IBM Integrated Security Solution for Cisco Networks. The role of this process is to provide the noncompliant client with a means to become compliant again and thus providing access to the network.

The remediation process is facilitated by the following components:

- Remediation handler

  The *remediation handler* initiates the remediation process. It receives the list of noncompliant settings from the compliance client, then asks the remediation server to provide the new software or the correct settings as required by the security policy. In the presented solution, each compliance check performed by the compliance agent is associated with a related *remediation object* that is capable of correcting the client posture if it is not compliant.

- Remediation server

  The *remediation server* provides the approved compliant settings templates for the clients. It listens to the clients' requests and responds to them. The response may include a number of elements, for example:

  - Installing the software package on the client
  - Starting or stopping a service on the client
  - Changing software settings on the client

- Remediation object

  The *remediation object* includes the required software and scripts required for the client to become compliant again. For example, the object for recovering from an outdated virus definition file would include the new virus definition file and would automatically install it.

  Depending on the conditions and security policy requirements, objects can be more or less complex.

Downloaded from www.Manualslib.com manuals search engine

2.2 Definition of a Network Admission Control project

Objectives of a Network Admission Control solution must be carefully planned because the result of having a large number of workstations quarantined may be more disruptive to the business than a particular virus attack.

Planning the Network Admission Control is an organizational challenge for most enterprises as it requires close cooperation among different groups of people in different roles, typically not closely related:

- Security officers responsible for the formal audit and compliance process
- Network administrators responsible for configuration of network devices
- Administrators responsible for everyday PC configuration and maintenance

It is essential to follow these steps in the implementation of the IBM Tivoli Security Compliance Manager and Cisco Network Admission Control:

- Creation of the policies to meet the business requirements and needs
- Building the policies on the compliance server
- Deploying the clients with the required software and initial policy
- Defining and implementing the remediation process
- Preparing the network infrastructure
- Turning on the security compliance enforcement

2.2.1 Phased rollout approach

Enforced Network Admission Control solutions are new to the industry and are not yet widely adopted so the phased approach to rollout is highly recommended.

In the first phase the most vulnerable network segments should be selected. These networks can be selected based on network topology knowledge or on the statistics from threat monitoring software.

NAC planning and deployment may be combined with the process of deploying wireless networks, along with IEEE 802.1x authentication.

Downloaded from www.Manualslib.com manuals search engine

Figure 2-5 illustrates a possible NAC deployment scenario.

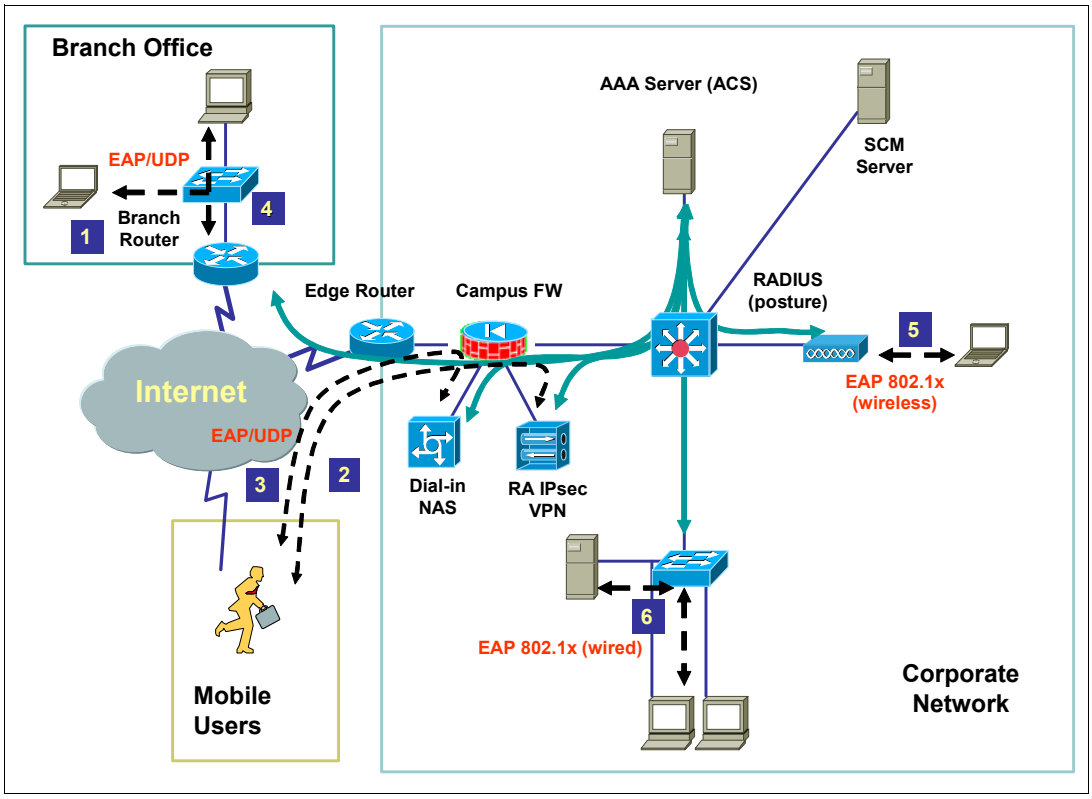


Figure 2-5 NAC deployment scenario

Typical candidates for NAC protection are networks (both wireless and wired) used by the mobile users to connect to the intranet while visiting the office [1], as well as the dial-up and VPN networks used to connect remotely [2,3]. (Especially in a dial-up and VPN environment, NAC enables posture control of the users (clients) connecting to the intranet where the other methods of enforcing compliance are limited.) In the next step, all branch office networks [4] can be protected with NAC. Finally, the solution can be extended to cover all wireless networks [5] and the stationary networks in the main campus [6].

A second factor strongly influencing project scope is the availability of automated remediation. As the number of quarantined clients increases, the number of help desk calls grows, raising the total cost of ownership (TCO) for the solution.

Downloaded from www.Manualslib.com manuals search engine

2.3 Design process

The MASS methodology that we follow in this book includes the following steps of the design process:

1. Model business process.
2. Establish security design objectives.
3. Select and enumerate subsystems.
4. Document conceptual security architecture.

We now walk through these steps.

2.3.1 Security compliance management business process

Figure 2-6 illustrates the *security compliance management business process*, which is described in detail in the redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450.

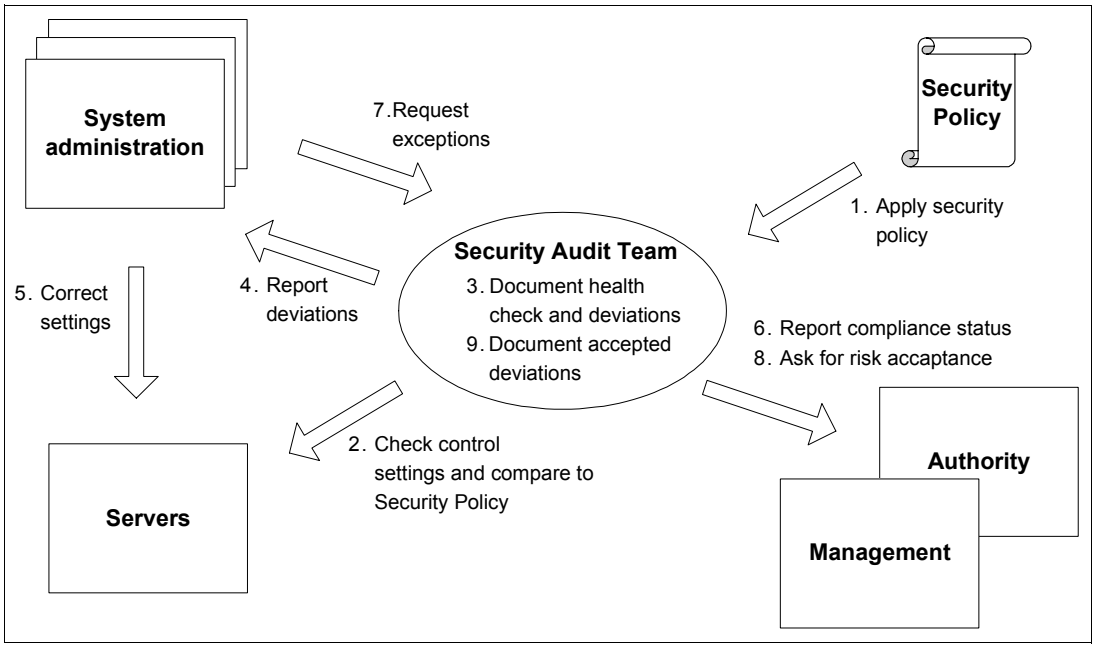


Figure 2-6 Generic security compliance management business process

The security compliance management business process consists of these general steps:

1. Apply security policy.

   The first step in setting up a health check process is to make sure that the required security control settings of the enterprise security policy are audited.

Downloaded from www.Manualslib.com manuals search engine

2. Check control settings and compare to security policy.

   The audit team periodically checks the systems to be sure their settings are in compliance with the policy. The audit team creates a report listing all controlled systems and the violated controls. Periodically the list also has to contain the complete security control settings and the systems that are controlled.

3. Document health check and deviations.

   The audit team archives the health check results documenting that the health check was performed according to the security policy.

4. Address deviations.

   The audit team has to inform the system owners and administrators about the health check process findings. Usually a list of deviations is handed over that specifies a target date for correcting the discrepancies.

5. Correct settings.

   The system administrators usually test the corrective actions in a test environment, verify that the system functions are not affected, and deploy the changes to the production environment.

6. Report compliance status.

   The audit team creates security compliance status reports for management and external audit purposes on a regular basis.

7. Request compliance exceptions.

   System administrators who come across security settings that affect the functionality of a system might request compliance exceptions. They ask the audit team whether the violation of a security control can be tolerated for a certain amount of time.

8. Ask for risk acceptance.

   When asked for compliance exceptions, the audit team will negotiate a risk acceptance with the management team. Usually, the risk acceptance is temporary until there is a secure solution for the IT system.

This process was designed for managing server compliance, where a typical environment includes a variety of different configurations, platforms, and applications. In a server environment, the number of application-specific deviations can be large and the change management process is required to correct any noncompliance.

On the other hand, in the typical workstation environment, all clients tend to be unified in terms of security settings, and the remediation process can be automated to enable faster accommodation to respond to security threats and avoid network infection.

Downloaded from www.Manualslib.com manuals search engine

The security compliance process for desktops and mobile clients can be simplified to look like this:

1. Apply security policy.

   The first step in setting up a health check process is to make sure the required security control settings of the enterprise security policy are audited.

2. Check control settings and compare to security policy.

   With the NAC in place the health check audit is automated and takes place every time the client connects to the network. This approach is very efficient in terms of protecting the network. However, additional security means may be required to protect the clients themselves (and information that they may contain) when they are operating outside the corporate network.

3. Address deviations.

   The system owner has to be informed about the findings of the health check process. Usually a list of deviations is presented to the user in a pop-up window and the noncompliant workstation is refused access to the corporate intranet.

4. Correct settings.

   As the configuration of the client tends to be unified and is regulated by a separate policy, there is no need to test the changes on every client. All requested changes should be applied as soon as possible either through the manual process according to designated instructions or in an automated way.

5. Report compliance status.

   The audit team creates security compliance status reports for management and external audit purposes on a regular basis. These reports document the number of noncompliances found, the progress of the new policy deployment, and so on.

2.3.2 Security policy life cycle management

In any organization, Information Technology resources are very important assets that are critical to business success and must be protected from unauthorized users without sacrificing integrity, availability, and confidentiality. Organizations must keep their IT security policies current and assess compliance regularly. Conducting regular security-education sessions for employees is a good idea.

The most important aspects of a security policy are identifying a threat, assessing the risk associated with it, providing means to protect critical data, and maintaining integrity and confidentiality without any compromise. Security policy creation is an ongoing process; all policies require constant review and amendment as necessary to suit the organization's business model. If for some

Downloaded from www.Manualslib.com manuals search engine

reason a policy cannot be complied with due to a particular business need, the situation has to be accepted as a security risk for a well-defined period of time and signed off by the project sponsor.

A policy that is created but is not enforced is no better than no security policy at all. This situation can expose the organization and put its credibility at stake.

We discuss more details of the full policy life cycle in the following sections. Figure 2-7 depicts the single steps in the security policy life cycle management process.

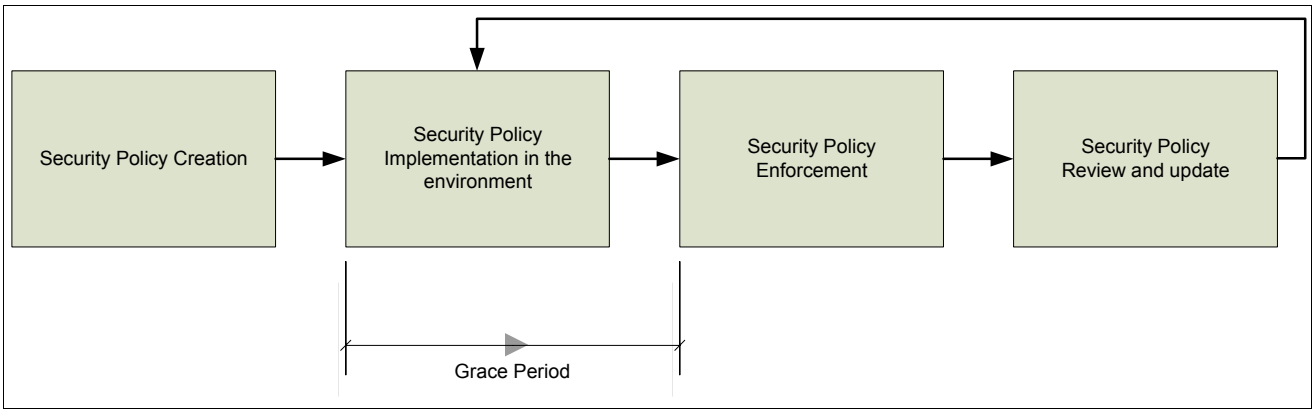


Figure 2-7 Security policy life cycle diagram

Creation

Chapter 1, “Business context” on page 3, discussed business reasons for having security policies in place. At this point we want to mention only that for the automated audit most of the policies have be operationalized. For example, the policy statement (such as “Each workstation connected to the corporate network should have all of the latest recommended security patches applied”) must be translated into a detailed list of all patches and hotfixes required for each operating system type.

This process is described in detail in the IBM Redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450.

Implementation

Establishing and implementing the policy in the environment typically are two separate processes involving different business units. IBM Tivoli Security Compliance Manager is an audit tool for automated verification of compliance. As part of the security audit process, it is not designed to perform any changes to the configuration of audited systems.

Downloaded from www.Manualslib.com manuals search engine

This means that for each desired change in the configuration settings, there must be an appropriate configuration change process in place to perform the changes on the afflicted systems. For example, if there is a security policy stating that each workstation must have antivirus software installed, there has to be a corresponding software installation process to distribute it to clients consistent with this policy.

Depending on the size of the environment, this can be achieved in a number of ways: fully automated, manually, or in some way in between. Depending on the type of policy, a different grace period for the implementation may be granted.

Enforcement

Before introducing the IBM Integrated Security Solution for Cisco Networks to the corporate environment, the only way to enforce the security policy as a client connected to the network was to perform a periodic audit of the configurations on individual user PC workstations. This was very ineffective and costly, the process was resource-intensive, and the results were not satisfactory. With the introduction of the IBM Integrated Security Solution for Cisco Networks, any noncompliant clients trying to connect to the network can be denied access to corporate resources or quarantined (that is, they are allowed to connect to only one designated network for remediation) until the workstation regains a compliant state according to the policies.

Review and update

As the IT environment and business requirements may change frequently, the security policy should be reviewed periodically and updated to reflect current security threats and business goals.

Updating the policy requires special attention because a *policy version* is the first value checked by the posture validation server in the IBM Integrated Security Solution for Cisco Networks. It is an important architectural decision whether clients with an outdated policy version should be admitted access to the compliance server to be updated or if first they should be updated using a remediation process and then, only if compliant, allowed to further access the network. This second approach is more secure, but it requires the automated remediation process to be operational.

2.3.3 Solution objectives

Several business drivers for the IBM Integrated Security Solution for Cisco Networks were described in 1.2, “Why we need this” on page 5. Each particular implementation may require all drivers to be in place or just a subset, so the selected objectives should be documented. The solution objectives will eventually drive most of the architectural decisions in the design process.

Downloaded from www.Manualslib.com manuals search engine

2.3.4 Network design discussion

In this section we discuss the following network design factors for the IBM Integrated Security Solution for Cisco Networks:

- Network segmentation via VLANs and downloadable IP ACLs
- Performance
- Adding new components that may not have been required previously

The IBM Integrated Security Solution for Cisco Networks introduces new zoning terminology for intranet networks:

Default network These are the network segments or virtual LANs (VLANs) to which clients are connected. Each client will be placed in a default network when they have been successfully admitted to the network.

Quarantine access This defines the resources that quarantined clients can access. These resources may be placed anywhere within the network but must be reachable by hosts that are in quarantine. Typical resources that are available while in quarantine are the remediation server, the compliance server, and public internet. In general, access to trusted networks is not allowed while in quarantine except in cases where the remediation or compliance servers are deployed within trusted networks.

Trusted network These are the parts of the network where the corporate resources are placed — domain servers, application and database servers, print servers, and so on. These network segments typically are not NAC-enabled as separate business processes govern the security compliance and configuration changes for servers. These segments are also not considered to be the serious source of threats to the rest of the network.

Default network

With Layer 3 NAC only networks connected to NAC-enabled routers can be isolated from other parts of the network. If existing network equipment has to be reused it may limit the number of possible untrusted network segments.

It is also important to realize that it is possible for a noncompliant client to connect to (and possibly harm) other clients connected to the same network segment. This limitation is addressed by Layer 2 NAC that can operate at network protocol layer 2 on switches, wireless access points (WAP), and virtual private network (VPN) concentrators.

Downloaded from www.Manualslib.com manuals search engine

In the reference architecture described later in this book, there are several untrusted networks that are the default networks to which users are assigned based on their identity-based authentication. When clients are in a healthy state, they should be placed in the default network based on the user's identity.

Quarantine access

We use this term to refer to the necessary network resources that a quarantined client needs to access. Network access is governed by the content of an *access control list* (ACL) applied to the router or switch port to which the client is connected, and this ACL may include several particular IP addresses required for remediation.

Depending on the solution design, remediation resources may include:

- Remediation server
- Compliance server
- Software distribution depot
- Internet access proxy

Trusted network

In a real world scenario this term is used for static, internal network segments where no clients are physically connected. In this book, we consider as trusted any network segment that is excluded from the NAC. Of course, other security means such as firewalls may still apply, but this outside the scope of this book.

Performance controls

Network admission control introduces the two timing parameters used to control solution behavior:

Revalidation period Defines how often the whole NAC procedure will be repeated for clients that are already connected.

Status query period Defines how often the posture agent is asked by the NAC router for changes in the posture. This second type of polling enables us to initiate a revalidation process if the client posture changes significantly (for example, if the user stops or disables an essential service required in the policy).

Depending on those settings the policy enforcement may be more or less rigid, but they also influence the end-user experience and network performance.

The revalidation process enables the client to pick up changes in a security policy version if no other distribution way is defined. However, as a result of the NAC process, a user connecting to the network is presented a pop-up window with the current status (Healthy, Quarantined, Checkup, Infected, or Unknown). If the

Downloaded from www.Manualslib.com manuals search engine

revalidation process takes place too often, this pop-up window may become annoying and significantly lower the user's productivity. The recommended value is 14400 seconds (4 hours) or more.

The router or the *network access device* (NAD) periodically queries the client for the current policy compliance status changes. This activity introduces additional network traffic, which becomes larger as the defined time intervals shorten. However, frequent polling enables quick disconnection from a client that becomes noncompliant from the network. Depending on the network architecture (number of clients connected to one NAD, network bandwidth, current network load, and so on) the status query period should not be shorter than 30 seconds.

2.4 Implementation flow

IBM best practice in implementation of this concept in an enterprise-wide deployment has been identified by the following project phases that would assist in a smooth transition to the new environment:

- Initiation
- Definition
- Design
- Build
- Maintenance

In the *initiation phase*, high-level project requirements are gathered and verified to be included in the Statement of Work (SoW) document.

During the *definition phase*, those requirements are refined and documented in detail, and as a result several of the documents are created, including *Project Definition Report* (PDR), *functional specification*, and *existing system analysis*.

In the *design phase*, the detailed design of the solution is created, typically in the form of architecture and design documents covering macro and micro design studies. Then the solution is actually implemented in the *build phase*.

The final stage is *maintaining and updating the solution* as the surrounding environment or business requirements change. This typically is a cyclic process as described in 2.3.2, "Security policy life cycle management" on page 30.

2.5 Scalability and high availability

Any architecture must be easily scalable and available at all times for secure and reliable business transactions and the future growth of the business. This

Downloaded from www.Manualslib.com manuals search engine

particular *security compliance concept* is aimed at validating client access to the corporate network, so it is mandatory that the system is available at all times.

As mentioned in Chapter 1, “Business context” on page 3, this concept can be deployed in stages, first targeting the most vulnerable user group (such as WLAN users) or a branch office, which may have a security exposure, and then being deployed across the whole enterprise. This concept is flexible, can be implemented with minimum required equipment, and can be scaled up to become a high-available solution as business demands.

If an existing infrastructure has all of the required components for Cisco Network Admission Control already in place, only a Tivoli Security Compliance Manager server and clients are to be deployed. This both protects the investment and provides an avenue to obtain additional benefits from the existing infrastructure. Similarly, if a Tivoli Security Compliance Manager server has already been deployed for server compliance control, it will be easier to use the existing Security Compliance Manager server and extend this concept to desktop workstations.

It is recommended that when this concept is deployed enterprise-wide, adequate redundancies for individual components are put in place. For example, a NAC-enabled Cisco router (Network Access Device) utilizes a secondary router that is configured in a redundant pair using *Hot Standby Routing Protocol* (HSRP), and Cisco Secure Access Control Servers are configured as a redundant pair in Active-Active or Active-Standby mode. These different devices and applications are explained in more detail in 3.1, “Logical components” on page 40.

If an organization has already deployed a Cisco Secure ACS v3.3 server for TACACS+ use, the same server can be utilized for the IBM Integrated Security Solution for Cisco Networks concept, thus safeguarding the existing investment. The size of your infrastructure load may become an issue for your Cisco Secure ACS. The Server will require an upgrade to Release 4.0 or later to support Layer 2 NAC.

Based on initial deployments, a single Security Compliance Manager Server V5.1 is capable of handling approximately 10,000 concurrent desktop clients. For the IBM Integrated Security Solution for Cisco Networks, the Security Compliance Manager server is not mission critical. It is required only for policy deployment and reporting.

For the manual remediation process, an existing infrastructure may be utilized (such as a download or update server that may be Web-based) for fixes and patches. Tivoli Provisioning Manager can be used to assist in the automation of the remediation process, taking advantage of its workflow capability.

Downloaded from www.Manualslib.com manuals search engine

Part 2, “Customer environment” on page 75, details a comprehensive deployment scenario.

2.6 Conclusion

In this chapter, we discussed the architecture and design principles for the IBM Integrated Security Solution using Cisco Networks. The overall architecture encompasses several components from IBM and Cisco, with integrated systems that complement each other by providing the first industry compliance-based Network Admission Control system with automated remediation capabilities.

The focus of this chapter was to introduce a description of functionality provided by the IBM Integrated Security Solution for Cisco Networks and how the IBM Tivoli products and Cisco NAC are integrated. We also discussed the high-level architecture and building blocks for the overall solution.

Designing the IBM Integrated Security Solution for Cisco Networks is a multi-phase process involving at least three groups of IT personnel. It is important to understand that this concept may have substantial influence on users’ experience and productivity, especially during the project rollout.

In the next chapter we provide the detailed description of the logical and physical components of the IBM Integrated Security Solution for Cisco Networks.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

3

Component structure

This chapter introduces the logical and physical components of the IBM Integrated Security Solution for Cisco Networks. The final section of this chapter talks about the logical data flow among the various components to better understand dependencies and component placement within the network.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

3.1 Logical components

The IBM Integrated Security Solution for Cisco Networks detects the state of network clients and compares it with a set of centrally defined and managed policies to establish client postures. It then dynamically reconfigures the network based on detected client postures and changes the state of devices to be in compliance with defined policies. This solution is an integration of products from IBM and Cisco. The IBM products focus on the aspects of compliance and remediation, and the Cisco products provide the Network Admission Control (NAC) and policy validation components.

This new integrated solution includes a set of policies and workflows that address certain well-known conditions such as operating system levels, hotfixes, and security and policy settings. These policies and workflows can be configured to address new instances of these conditions. The IBM Integrated Security Solution for Cisco Networks is an extensible offering that provides the ability to create new policies to detect various combinations of device postures and workflows that can remediate various states on these devices. This can provide you with the flexibility to define polices that are unique to your environment.

The solution integrates three major independent logical components or subsystems with add-on components specifically developed for the IBM Integrated Security Solution for Cisco Networks, depicted in Figure 3-1.

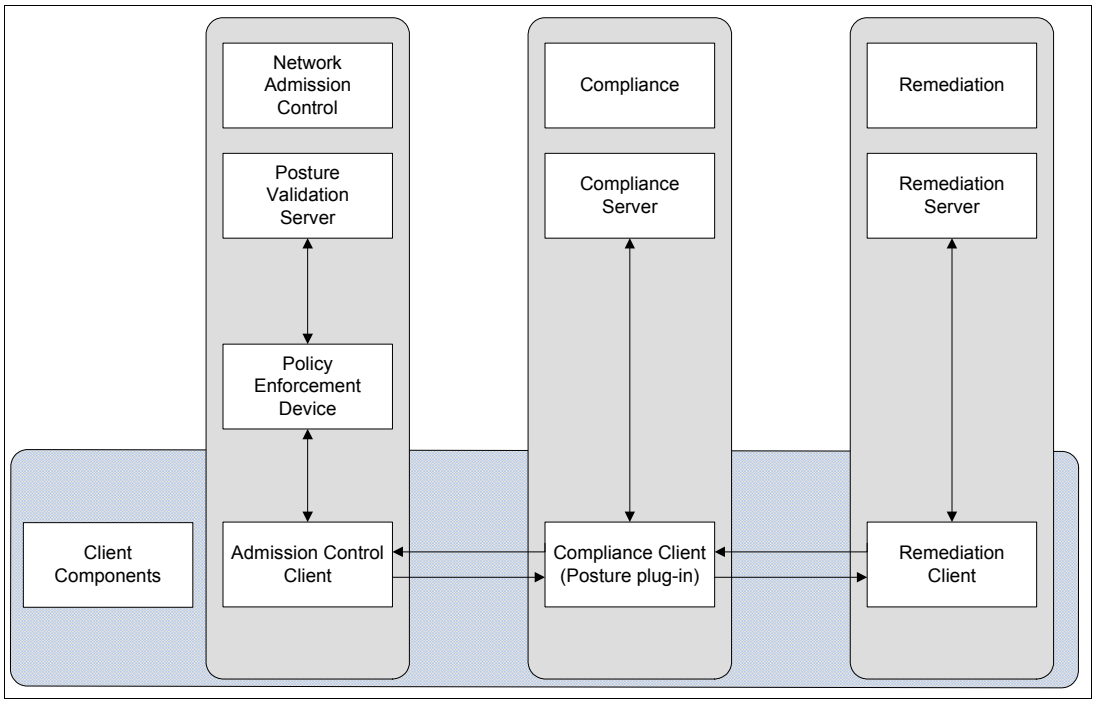


Figure 3-1 Solution logical block diagram

Downloaded from www.Manualslib.com manuals search engine

The logical components are:

- Network Admission Control
- Compliance
- Remediation

The following sections provide function and architecture details for each component.

3.1.1 Network Admission Control

Network Admission Control (NAC) is the Cisco component of the solution that provides enforcement by restricting traffic based on the client's posture. Cisco NAC can be implemented via NAC Framework or NAC Appliance. NAC Framework provides NAC functionality within the infrastructure, posturing at the network access device, where as NAC Appliance provides posturing on an appliance. Both NAC Framework and NAC Appliance can be integrated simultaneously into the network. An overview introducing the concepts of NAC Framework and NAC Appliance can be found in Appendix B, “Network Admission Control” on page 471.

Network Admission Control Framework

The Network Admission Control Framework consists of the following subcomponents:

- Posture validation server
- Policy enforcement device
- Admission control client

Posture validation server

The *posture validation server* validates the client posture against network access policy. In our solution the Cisco Secure Access Control Server (ACS) acts as the posture validation server. The Cisco Secure ACS performs these functions:

- It enables administrators to create polices that are used as validation criteria for clients trying to access the network.
- It validates the security posture credentials received from a client machine. The validation process compares the client’s current posture with a predefined desired posture.
- It forwards the appropriate network access policy for the client to a network access device, such as a switch, router, VPN concentrator, Adaptive Security Appliance or access point, to restrict traffic flow based on the client’s posture.

The Cisco Secure ACS is an *authentication, authorization, accounting* (AAA) server that provides a centralized authentication and policy deployment platform

Downloaded from www.Manualslib.com manuals search engine

for network devices and other services. The various components that constitute the ACS and a brief description of their functions are discussed here.

The ACS architecture consists of seven services bundled within ACS. Figure 3-2 shows the internal ACS components and their functions.

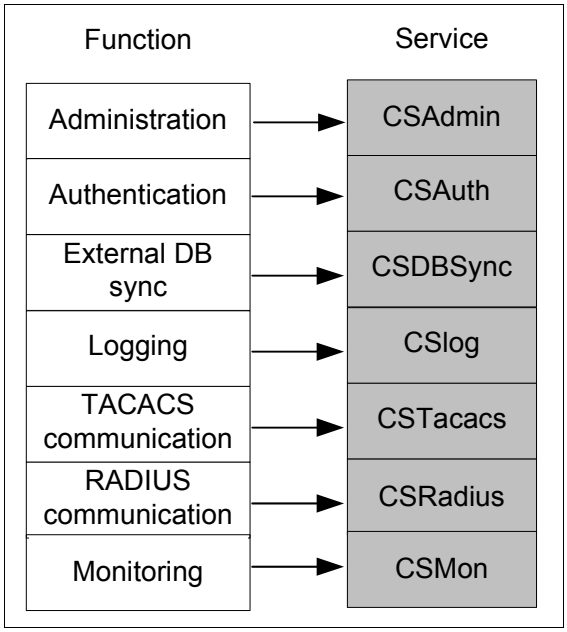


Figure 3-2 ACS architecture

Here are brief explanations for the ACS services:

CSAdmin Provides an HTML interface for administration of ACS

CSAuth Provides authentication services

CSDBSync Provides synchronization of the internal ACS user database with third-party external RDBMS applications

CSlog Provides logging services both for accounting and system activity

CSTacacs Provides communication between TACACS+ AAA clients and the CSAuth service

CSRadius Provides communication between RADIUS AAA clients and the CSAuth service

CSMon Provides monitoring, recording, and notification of ACS performance and includes automatic response to some scenarios

Downloaded from www.Manualslib.com manuals search engine

Note: For more information about the ACS architecture and administration refer to the ACS user guide and ACS administration guides at the Cisco Web site:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/tsd_products_support_series_home.html

Policy enforcement device

Clients access enterprise resources via the network which makes it an effective point to validate system posture prior to allowing access to such resources. In the NAC solution, policy enforcement is accomplished using a network access device that has the NAC feature set enabled in Cisco IOS (Internetworking Operating System). The network access device also acts as a client to ACS which provides it with direction on how to handle connected devices.The functions of policy enforcement devices are:

- The NAD demands endpoint posture *credentials* from the network-attached client through a client software component. This information is relayed to ACS for an admission decision.
- Based on appropriate network access policy provided by ACS, the NAD permits, denies, or restricts the network access of the network client.
- The NAD also checks for a change in posture of the client by polling the client at specified intervals.

Admission control client

The Cisco Trust Agent is a specialized application that runs on network clients. It collects security posture information from the NAC-compliant applications that are installed on network clients and reports the posture information to a posture validation server, which is the Cisco Secure ACS. For the IBM Integrated Security Solution for Cisco Networks, the posture information is provided by the Tivoli Security Compliance Manager client. Based on the reported security posture, the network client is either permitted, denied, or allowed restricted access to the network.

Downloaded from www.Manualslib.com manuals search engine

Figure 3-3 shows the Cisco Trust Agent architecture, followed by a brief explanation of the components that make up the Cisco Trust Agent.

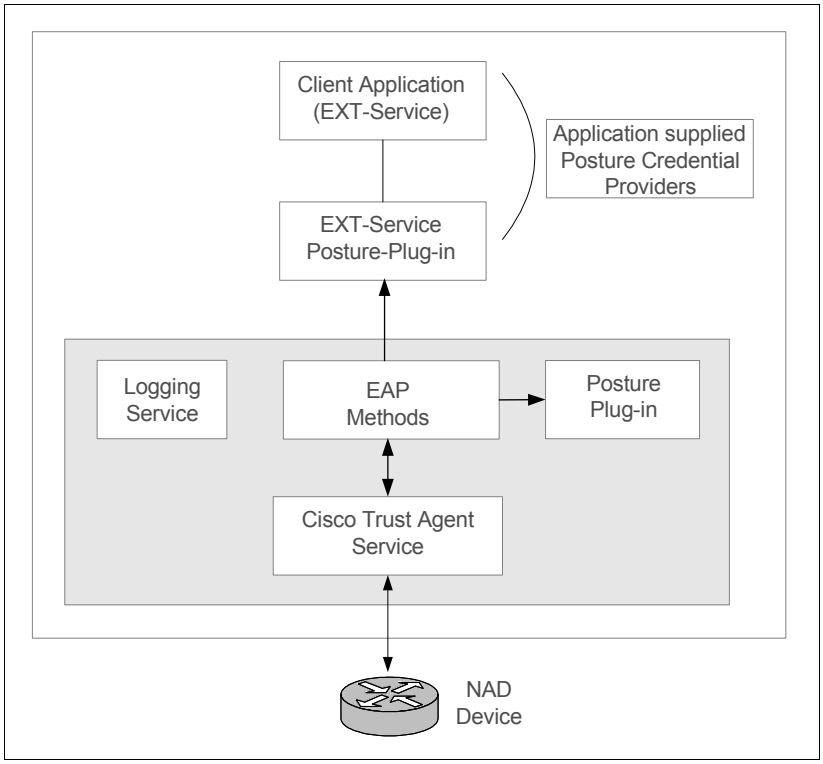


Figure 3-3 Cisco Trust Agent architecture

Cisco Trust Agent service Responds to network requests for client system posture information.

Logging service Logs event information received from Cisco Trust Agent components and from NAC-compliant applications into log files.

Posture plug-in Provides the capability to collect information such as operating system type and version.

EXT-Posture plug-in Represents an external or third-party posture plug-in. This is a communication path provided by Cisco Trust Agent software to enable system integrators to pass posture information to the Cisco Trust Agent. For IBM Integrated Security Solution for Cisco Networks, an IBM-developed posture plug-in communicates with Cisco Trust Agent and provides posture credentials.

Downloaded from www.Manualslib.com manuals search engine

EAP methods	Provide a mechanism to authenticate the application or device requesting the host credentials, and encrypts or decrypts that information.

Network Admission Control Appliance

The Network Admission Control Appliance consists of the following subcomponents:

- Clean Access Manager (CAM)
- Clean Access Server (CAS)
- Clean Access Agent (CAA)
- Clean Access Policy Updates

Clean Access Manager (CAM)

The Clean Access Manager is the administration server and database that centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. The Web admin console for the Clean Access Manager is a secure, browser-based management interface. For out-of-band (OOB) deployment, the Web admin console provides the Switch Management module to add and control switches in the Clean Access Manager's domain and configure switch ports.

Clean Access Server (CAS)

The Clean Access Server is the gateway between an untrusted and a trusted network. The CAS enforces the policies you have defined in the CAM Web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and NAC Appliance system requirements. It can be deployed *in-band* (always inline with user traffic) or *out-of-band* (inline with user traffic only during authentication/posture assessment). It can also be deployed in Layer-2 mode (users are L2-adjacent to CAS) or Layer-3 (users are multiple L3 hops away from the CAS) mode.

Clean Access Agent (CAA)

When enabled for your Cisco NAC Appliance deployment, the Clean Access Agent can ensure that computers accessing your network meet the system requirements you specify. The Clean Access Agent is a free, read-only, easy-to-use, small-footprint program that resides on user machines. When a user attempts to access the network, the Clean Access Agent checks the client system for the software you require, and helps users acquire any missing updates or software.

Agent users who fail the system checks can be assigned to the *temporary* role. This role gives users limited network access to the resources needed to comply with the Clean Access Agent requirements. Once a client system meets the requirements, it is considered *clean* and allowed network access.

Downloaded from www.Manualslib.com manuals search engine

Clean Access Policy Updates

These are regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software.

3.1.2 Compliance

Tivoli Security Compliance Manager, a a client/server-based policy compliance solution, supports the definition of policies that specify conditions that should exist on a client, detects the state of these conditions and stores the collected current state information on the server. Security Compliance Manager collectors are written to evaluate system data and state information. Collectors can be written to evaluate virtually any system parameter.

Compliance server

The server is the central component of a Security Compliance Manager infrastructure. The server's responsibilities include:

- Creating and deploying new policies
- Determining what security compliance data is collected and how to interpret the data using the compliance management components
- Managing security compliance data collection frequency and grouping of policies for different types of user groups
- Storing the security compliance data received from the clients and providing the available data to users through the administration console and administration commands
- Providing security violation details as a basis for the compliance report components

Downloaded from www.Manualslib.com manuals search engine

Figure 3-4 depicts Security Compliance Manager's high-level component architecture, followed by a brief explanation.

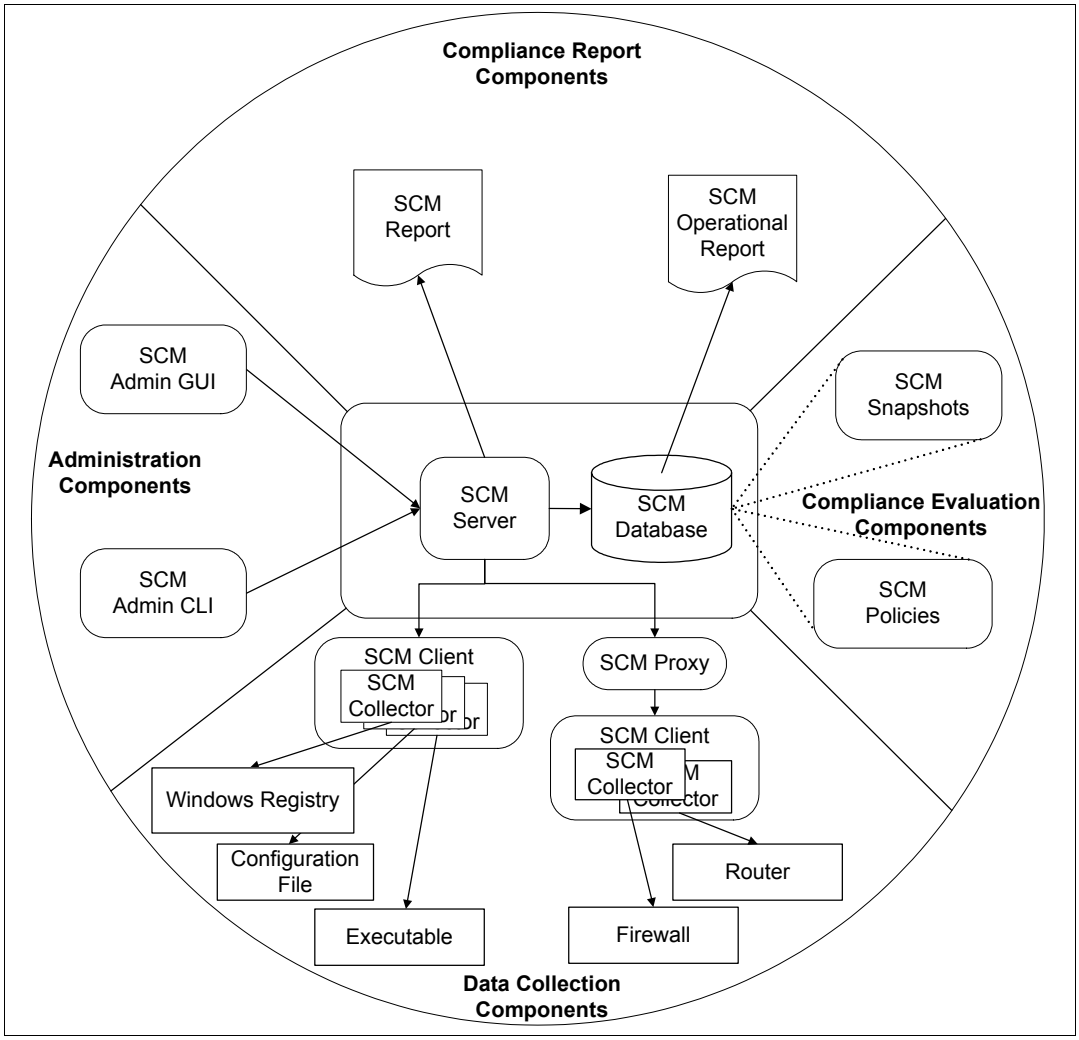


Figure 3-4 IBM Tivoli Security Compliance Manager logical component architecture

Figure 3-4 shows:

Administration components Consist of a graphical user interface and a command line interface (CLI). Used to manage the Security Compliance Manager components.

Data collection component Build a framework for collecting security-relevant configuration data from connected systems such as operating systems, middleware components, applications, firewalls, routers, and so on.

Compliance reporting Deliver different kinds of configurable reports for audit purposes and correcting deviations.

Downloaded from www.Manualslib.com manuals search engine

Compliance evaluation	Consisting of Security Compliance Manager snapshots and policies, these components centrally verify security compliance.

Note: You can find more details about these components in the IBM Redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450.

Compliance client

The client consists of modules that run on the endpoint to collect compliance information and report it to the Security Compliance Manager server. In the IBM Integrated Security Solution for Cisco Networks, the Security Compliance Manager client introduces a new posture plug-in that communicates with the Cisco Trust Agent required by Cisco to report posture data during the NAC process.

The Security Compliance Manager client is Java™-based software that runs on systems to be monitored for security compliance. By default, the client runs as a daemon with root authority on UNIX® systems, or as a service running under the local system account on Microsoft® Windows® systems. The client provides the runtime environment for collectors deployed to the system and handles communication with the server.

Downloaded from www.Manualslib.com manuals search engine

The compliance client component (Figure 3-5) consists of the following modules:

- Policy collector
- Posture collector
- Posture cache
- Posture plug-in
- Default remediation handler

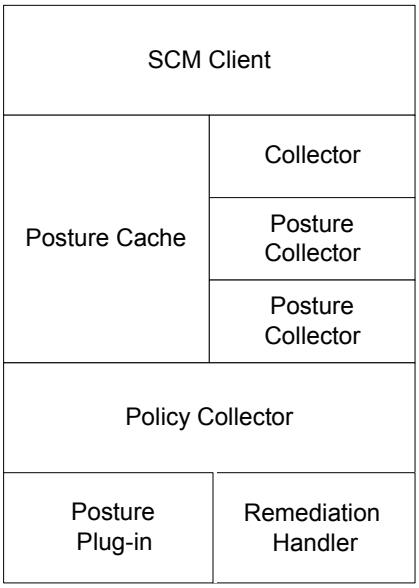


Figure 3-5 Compliance client logical component

Posture collector

A collector is a Java language-based software module, packaged as a Java Archive (JAR) file, that collects specific information from a client system. The collector may use different methods for collecting data depending on the compliance data to be gathered. Here are some examples:

- Reading the content of one or more files on the client system
- Running an operating system command or utility and examining the output
- Running an executable program packaged as part of the collector JAR file and examining the output
- Reading information from the registry on Windows systems

In a scenario where an organization is using a Security Compliance Manager solution independently, collectors are called *Security Compliance Manager collectors*. In this scenario, an Security Compliance Manager collector collects compliance information and *only* reports it to the Security Compliance Manager server.

Downloaded from www.Manualslib.com manuals search engine

In the IBM Integrated Security Solution for Cisco Networks, the collector is called a *posture collector*. A posture collector consists of posture data collection and posture status determination. The posture data collection part of a posture collector is the same as in a regular Security Compliance Manager collector, but the posture status determination part of a posture collector is an extension to the standard model. A posture collector determines the client posture status by checking or comparing a *collected value* with a *required value*. The required posture data value, which is part of the collector, is inserted into the collector by editing collector parameters while creating a collector on the Security Compliance Manager server.

If required posture data values are null in the parameters, the posture determination part is not executed. Each posture collector stores into the posture cache:

- Collected posture data
- Posture status, which is from the set {PASS, FAIL, WARN, ERROR}
- Optional posture messages
- Zero or more remediation actions

The posture collector also contains appropriate information to be used in order to remediate any compliance violations.

A posture collector can be called by the Security Compliance Manager server or by the policy collector on the client, or it can be scheduled.

Note: Organizations having Security Compliance Manager deployed can use Security Compliance Manager collectors and posture collectors at the same time, but only posture collectors can trigger posture violations and hence trigger NAC enforcement. To enforce a compliance policy before a client connects to the enterprise network, posture collectors have to be deployed using the IBM Integrated Security Solution for Cisco Networks.

Policy collector

After a posture collector collects all required information from the client system, the policy collector counts the number of posture collector results that show noncompliance; this result forms the *violation count*. The violation count and the policy collector's version information together form the *posture credentials*. The policy collector also receives back the client's posture that is evaluated by the posture validation server (ACS). Depending on the client's posture status, the policy collector calls the default *remediation handler* to present information about noncompliant items on the client system to the end user.

Downloaded from www.Manualslib.com manuals search engine

Posture cache

This component provides the caching area where posture collectors store the results of posture determination in a temporary file. The policy collector refers to the information captured in the posture cache for determining the violation count.

Posture plug-in

Posture plug-ins are the means by which the Cisco Trust Agent requests and receives security posture information from NAC-compliant applications installed on the system.

Default remediation handler

The *default remediation handler* provides a graphical interface for displaying the compliance posture data and a method for reinitiating the compliance scanning process. The default remediation handler supports the passing of noncompliance data and remediation request data to the remediation client.

3.1.3 Remediation

The compliance component identifies and reports policy violations. To make the client productive again, these violations must be mapped to corresponding corrective actions that are provided through a remediation subsystem. This remediation subsystem provides a set of software and configuration management capabilities that an enterprise can leverage to centrally manage and automate the remediation process for noncompliant endpoints.

The remediation subsystem consists of a remediation server and the remediation client.

Remediation server

IBM Tivoli Configuration Manager can automate the manual tasks of installing software and updating configurations on endpoints. It enables an enterprise to centrally manage and automate software and configuration for endpoints.

For our solution, Tivoli Configuration Manager helps automate the remediation of noncompliant endpoints by installing required software updates or correcting configuration issues. Its remediation capabilities include software levels, typically operating system levels and fix packs, patch levels, virus and firewall updates, last virus scans history, password strength and history, and policy level.

Outside the IBM Integrated Security Solution for Cisco Networks environment, Tivoli Configuration Manager uses the *Tivoli Framework* to monitor software levels on clients, manage remediation content in self-installing objects, and perform a number of other functions. In the IBM Integrated Security Solution for Cisco Networks, requests for the required corrections are initiated by the client,

Downloaded from www.Manualslib.com manuals search engine

and any client components that would normally be installed on a Tivoli Configuration Manager client are embedded within the Security Compliance Manager Compliance policy.

For the IBM Integrated Security Solution for Cisco Networks, the Tivoli Configuration Manager Software Distribution Server and Web Gateway components are used. The Software Distribution server is extended with administrative utilities that support the creation of remediation objects that are designed to be invoked and installed based on requests from the compliance client. These utilities also publish the remediation objects to the Web Gateway. The Web Gateway is extended with a *Remediation Servlet* that is designed to accept the remediation requests from the client and provide the appropriate remediation objects in response to these requests.

Remediation handler component

The *remediation handler* is a specific component for the IBM Integrated Security Solution for Cisco Networks that handles the interface between the Security Compliance Manager client for NAC and the Tivoli Configuration Manager server. These components are shown in Figure 3-6 on page 56 and explained in the next sections. This component is not actually installed on the client. Instead, it is embedded into compliance policies as a special collector and is downloaded to the clients as part of the compliance policy.

3.2 Physical components

The discussion so far has been focused on the various logical components that make up the IBM Integrated Security Solution for Cisco Networks. In this section we map the logical components into physical components that make up the IBM Integrated Security Solution for Cisco Networks. The physical components of the solution can be categorized into three types: client components, network components, and server components. All three components work together to effectively deploy polices that an enterprise would like to implement.

3.2.1 Network client

A network client is the end device that must comply with the policy. The client in the current context of the solution can be a PC or mobile computer running Windows 2000, Windows XP, or Windows NT®, and Red Hat Linux® Enterprise Linux 3.x and 4.0. The network client must have the following software components installed:

- Cisco Trust Agent client software
- Security Compliance Manager client

Downloaded from www.Manualslib.com manuals search engine

Cisco Trust Agent

The Cisco Trust Agent is Cisco client software that is required to pass posture credentials and validation results between the Cisco NAC solution and the IBM Security Compliance Manager client.

Security Compliance Manager client

The Security Compliance Manager client is a software component that is physically installed on the network client. It is responsible for communicating with the Security Compliance Manager Server to keep the client's policy up-to-date and to send collected compliance data to the server where it is stored in a database.

Security Compliance Manager policy

A Security Compliance Manager policy containing all of the collectors that will be run on the client is downloaded to clients and is the essential unit that performs most of the work on the client. Policies contain many collectors, each of which is responsible for collecting an explicit set of data.

Special *posture collectors* contain parameters that describe the required values for various data and remediation information to be provided to the remediation handler when collected values do not match required values.

A special *policy collector* gathers data from the various collectors and summarizes the collector data to provide version information (for example, software version of Security Compliance Manager client) and the number of policy violations to the Cisco Trust Agent client software. Communication between the Cisco Trust Agent client and Security Compliance Manager client is implemented using a plug-in developed by IBM.

Tip: A personal firewall and Host IDS running on the client systems are recommended for controlling traffic and alerting of intrusions on the client. The Cisco Security Agent provides endpoint server and desktop protection against new and emerging threats due to malicious network activity. The Cisco Security Agent identifies and prevents malicious behavior resulting in the elimination of known and unknown, or "Day Zero," network threats. The Cisco Security Agent provides for the aggregation and extension of multiple endpoint security functions by providing intrusion prevention and distributed firewall capabilities in addition to malicious mobile code protection, system integrity assurance, and audit log consolidation. Read more about this product at:

http://www.cisco.com/go/csa

Downloaded from www.Manualslib.com manuals search engine

3.2.2 Network access infrastructure

All users connect to enterprise resources via network access devices. The topology varies depending on the size of the organization, but most networks can be classified into LAN (local area network), WAN (wide area network), or remote access. The LAN enables connectivity to users within a location. A WAN provides connectivity to remote or branch office users who need connectivity to resources that are centrally deployed. Remote access users access the enterprise resources using dial-up or the Internet to connect. Virtual private network (VPN) technology is generally deployed for remote access secure connectivity. VPN connectivity is also used by remote and branch offices to provide a low-cost secure access method. Enterprise users may use any of these methods to access the enterprise resources.

Network access device

In the IBM Integrated Security Solution for Cisco Networks, the network enforces the policy, so the network access device (NAD) becomes an integral part of the solution. In our solution, Cisco switches, routers, VPN Concentrators, Adaptive Security Appliances, and access points can be used as policy enforcement devices.

Note: Refer to the Cisco Web site for the latest list of supported hardware and corresponding software for the NAC solution at:

`http://www.cisco.com/go/nac`

3.2.3 IBM Integrated Security Solution for Cisco Networks servers

The servers are a set of centrally administered devices that enable creation, deployment, and management of policies. They also provide a platform for centralized validation and reporting.

Cisco Secure Access Control Server

The Cisco Secure Access Control Server (ACS) is a Cisco AAA server or an ACS appliance that provides posture validation to the client. Posture credentials of the client are then validated and network access is provided to clients depending on the policy and their posture status. The ACS delivers network policy information such as ACL and RADIUS parameters to the NAD that enforces the policy.

Security Compliance Manager server

The Security Compliance Manager server is an IBM-developed solution for the complex problem of deploying and checking enterprise polices. The server provides a platform for the creation of various client compliance policies that can

Downloaded from www.Manualslib.com manuals search engine

be deployed to the clients. The server is also used for administration and for providing reports about client compliance to deployed policies.

Tivoli Configuration Manager servers

There are two Tivoli Configuration Manager servers used for remediation. Tivoli Configuration Manager Software Distribution Server is used to create remediation objects and publish them to the Tivoli Configuration Manager Web Gateway Server, where they are made available to clients requesting remediation.

3.3 Solution data and communication flow

Until now we have discussed the various components of our solution. This section explains the communication and data flow and how the various components integrate when the solution is being deployed.

Note: This section describes the NAC Framework solution. A similar description of the NAC Appliance solution is in Appendix A, “Hints and tips” on page 441.

Downloaded from www.Manualslib.com manuals search engine

The flow consists of these process groups, depicted in Figure 3-6:

1. Policy creation and deployment
2. Posture collection
3. Posture validation and policy enforcement
4. Remediation

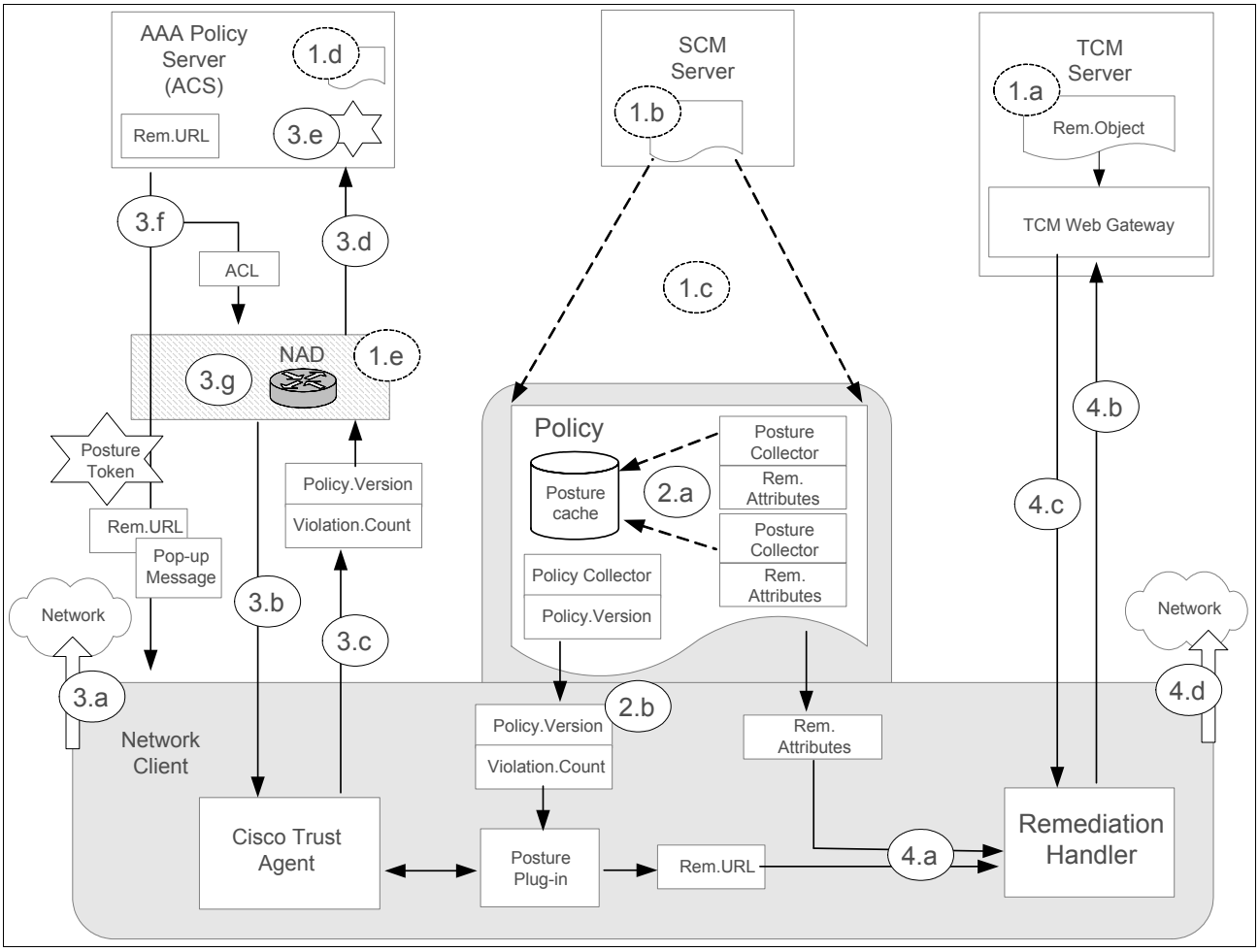


Figure 3-6 Solution data and communication flow

The naming convention in the diagram has four flows based on the process.

Policy creation and deployment (flow 1)

The first step in the data flow is the creation and deployment of a policy. If a Tivoli Configuration Manager server is used for remediation, a corresponding

Downloaded from www.Manualslib.com manuals search engine

remediation object should also be provided. Details of the policy creation and deployment process are discussed here:

- Remediation object creation and publishing (1a)

  A *remediation object* that can remediate violations must be provided. The naming and creation of these objects is dependent on the corresponding Security Compliance Manager posture collectors and certain naming conventions. For example, posture collectors that check for hotfixes will have a different name mapping than those that check for local system settings, and the remediation objects that will be created for these collectors must take this name mapping into account. Details on naming conventions and the creation and publishing of remediation objects are provided in 8.2.4, “Installation of the Software Package Utilities” on page 394.

- Compliance policy creation (1b)

  A *compliance policy* must be created or updated on the Security Compliance Manager server. The policy may include:

  – *Posture collectors* of appropriate types to detect violations

  – The collectors’ parameters, which must be configured with the values that will be checked against when making compliance decisions

  – Information specific to the remediation object that will remediate violations when detected as noted in step 1a

  – Other attributes that are used to support automated remediation

  Each policy must include a *policy collector*, which must have its collector parameters updated for Policy_Version. The new value must be noted for entry in the ACS policy.

  Be aware that only a single policy containing the policy collector can be deployed to a client. You can define multiple Security Compliance Manager policies, each with a policy collector instance, but you should never assign more than one of these policies to a group (and thus a client).

- Policy deployment (1c)

  Security Compliance Manager provides a means to deploy the policy file to the client, which requires that the client has direct access to the Security Compliance Manager server. Whenever a client is in communication with the server, the appropriate policy updates are automatically downloaded to the client. Our reference architecture provides for the Security Compliance Manager client to be in contact with the Security Compliance Manager Server regardless of whether it is being quarantined, which will allow quarantined clients to download required policy updates using the standard Security Compliance Manager method.

Downloaded from www.Manualslib.com manuals search engine

- Cisco Secure ACS policy creation (1d)

  An ACS policy consists of rules that must match required posture criteria. Depending on the matched criteria, a token is assigned to the network client that requires validation. The token results in the network client being dynamically assigned to a group. Based on the *Network Access Profiles* configured on the ACS, the group has an access policy (for example, an ACL or a RAC) associated with it. Thus depending on the client's posture, the ACS assigns an access policy to the client that is enforced by the NAD.

  An example of such *posture criteria* in our solution is to match the OS type, the Security Compliance Manager Policy_Version noted in step 1b, and the violation count to a predetermined value defined by the enterprise policy. This criteria must be deployed as a policy on the ACS. The ACS policy also has a feature to provide an action parameter with each rule. Whenever a new Security Compliance Manager policy is deployed, the ACS Server's policy must be updated with the new Policy_Version as noted at the Security Compliance Manager server in 1b.

- NAD configuration deployment (1e)

  The NAD should be a NAC-compliant hardware device with specific software that supports NAC. It has to be deployed at the appropriate network points. The NAD must be deployed with a NAC-related configuration.

Posture collection process (flow 2)

After the policy has been deployed in the various subsystems, the next step is to collect the posture compliance from the clients. This is the posture collection process:

- Posture collection (2a)

  The policy that has been deployed to the clients in process 1c includes posture collectors that are responsible for determining the client's posture. The posture collector determines the client's posture status by comparing the required posture data value with collected posture data.This data is stored in the posture cache.

- Violation count (2b)

  The policy collector determines the number of violations. The number of violations and the policy collector version, which form the posture credentials, are passed on to the Cisco Trust Agent when it queries the Security Compliance Manager client. The policy collector passes the posture credentials to the Cisco Trust Agent using a posture plug-in.

Downloaded from www.Manualslib.com manuals search engine

Posture validation and policy enforcement (flow 3)

This section contains details about how a client in a live environment connects to the network and how its posture is validated by the ACS. After validation the client is provided access based on client posture.

- Client network access (3a)

  The network client initiates IP traffic that crosses a NAC-enabled route point or connects to a switch running 802.1X. The NAD initiates an EAP session, forwarding the EAP identity of the NAC-client computer to Cisco Secure ACS. The ACS initiates a PEAP (Protected Extensible Authentication Protocol) session with the NAC-client computer, so that all NAC communications are encrypted and trusted.

- Posture query (3b)

  If various conditions are met, the NAD initiates posture validation. The NAD applies a default access policy to the client network traffic and initiates an EAP session with the client. The NAD queries the client for posture credentials.

- Posture status reply (Cisco Trust Agent - NAD) (3c)

  The Cisco Trust Agent, running on the network client, receives the security posture credential request and in turn requests security posture credentials from the NAC-compliant applications (in this case, Security Compliance Manager client). The security posture credentials are requested and received through posture plug-ins provided by IBM. When the Cisco Trust Agent queries for posture credentials, the Security Compliance Manager client component responds with the posture credentials that were collected in 2b. The Cisco Trust Agent sends this information to the NAD.

- Posture status reply (NAD - ACS) (3d)

  The NAD transfers the posture credentials to the Cisco Secure ACS using EAP over RADIUS (EAPoRADIUS).

- Posture evaluation (3e)

  Cisco Secure ACS evaluates the security posture credentials using rules in the local database. The result of the evaluation is an *application posture token*. If applications are used other than Security Compliance Manager, there could be multiple application posture tokens.

  Cisco Secure ACS consolidates the application posture tokens into an overall *system posture token*. The system posture token is typically the worst-case scenario for all application posture tokens. The system posture token can have one of the following values:

  – Healthy
  – Checkup

Downloaded from www.Manualslib.com manuals search engine

- Quarantine
- Infected
- Unknown

- Posture notification (3f)

  After the ACS has determined the posture token it performs these actions:

  a. Cisco Secure ACS sends the system posture token to the network client.

  b. The Cisco Secure ACS sends the network client an action to be taken that is the result of the client being assigned to a group complying to a particular policy level. If a customer uses the IBM Integrated Security Solution for Cisco Networks with Configuration Manager integration and the client happens to get a token “quarantine,” the results parameter will be the *remediation URL* pointing to the Configuration Manager server.

  c. Cisco Secure ACS sends the NAD device the RADIUS attributes as configured in the mapped user group, including ACLs or RACs as per network access policy and attribute-value pairs. The optional user notification can be used to display meaningful messages to the client that correspond to the posture token assigned to the network client. The access policy depends on the policy defined by the organization’s network policy.

  d. When the Cisco Secure ACS sends the system posture token to the NAC-client computer, the ACS ends the PEAP session with the client.

  e. Cisco Secure ACS logs the results of the posture validation request.

- Network policy enforcement (3g)

  The NAD device enforces network access as dictated by Cisco Secure ACS in its RADIUS response. By configuring group mapping, you define authorizations and, therefore, network access control, based on the system posture token determined as a result of posture evaluation.

  To fully control what resources users have access to under all conditions, a mapping of default user groups, posture tokens, and access restrictions is specified in ACS. In general, each user will be assigned to a default user group based on his authentication. Each user group is mapped to several posture tokens, and each combination of user group to posture token can be assigned either a RADIUS Access Control set or a downloadable IP ACL filter.

Downloaded from www.Manualslib.com manuals search engine

Remediation (flow 4)

Two cases should be considered for the remediation process: one where the organization has a Tivoli Configuration Manager server with an automatic remediation implementation, and the other where the organization will use manual methods for remediation using a Web server or alternative methods. Manual remediation could be provided with a Web server where a user can download the required software to meet the software compliance requirements and manually comply to configuration requirements.

In the case of automatic remediation, these processes result in remediation:

- Remediation request (4a)

  The token received in step 3e determines the posture of the client. If the client receives a *quarantine posture* this requires being provided with remediation, (for example, a corrective action). The remediation is initiated by the user of the network client machine by clicking a remediation button from the Security Compliance Manager client pop-up window. The *policy collector* then passes a *remediation URL* and a remediation request containing the name of the remediation object for remediating policy objects to the *remediation handler* on the network client.

- Remediation execution (4b)

  The *remediation handler* on the network client contacts the Configuration Manager Web Gateway server requesting remediation. An appropriate object is downloaded and executed and the client is remediated.

- Network access (4c)

  The NAD continuously polls the client for change in posture status. If the network client has been remediated, it has to go through the process steps 2a through 3g again. After the network client is remediated of all violations, it receives a *healthy token* from the ACS and the access control policy is changed in the NAD device. At this point the client is compliant to the enterprise policy and is provided access to the enterprise network.

Downloaded from www.Manualslib.com manuals search engine

3.3.1 Secure communication

The components are designed to provide a high level of security between the various elements in the solution. We provide a description of how the various components securely communicate, and Figure 3-7 shows an overview of the secure communications.

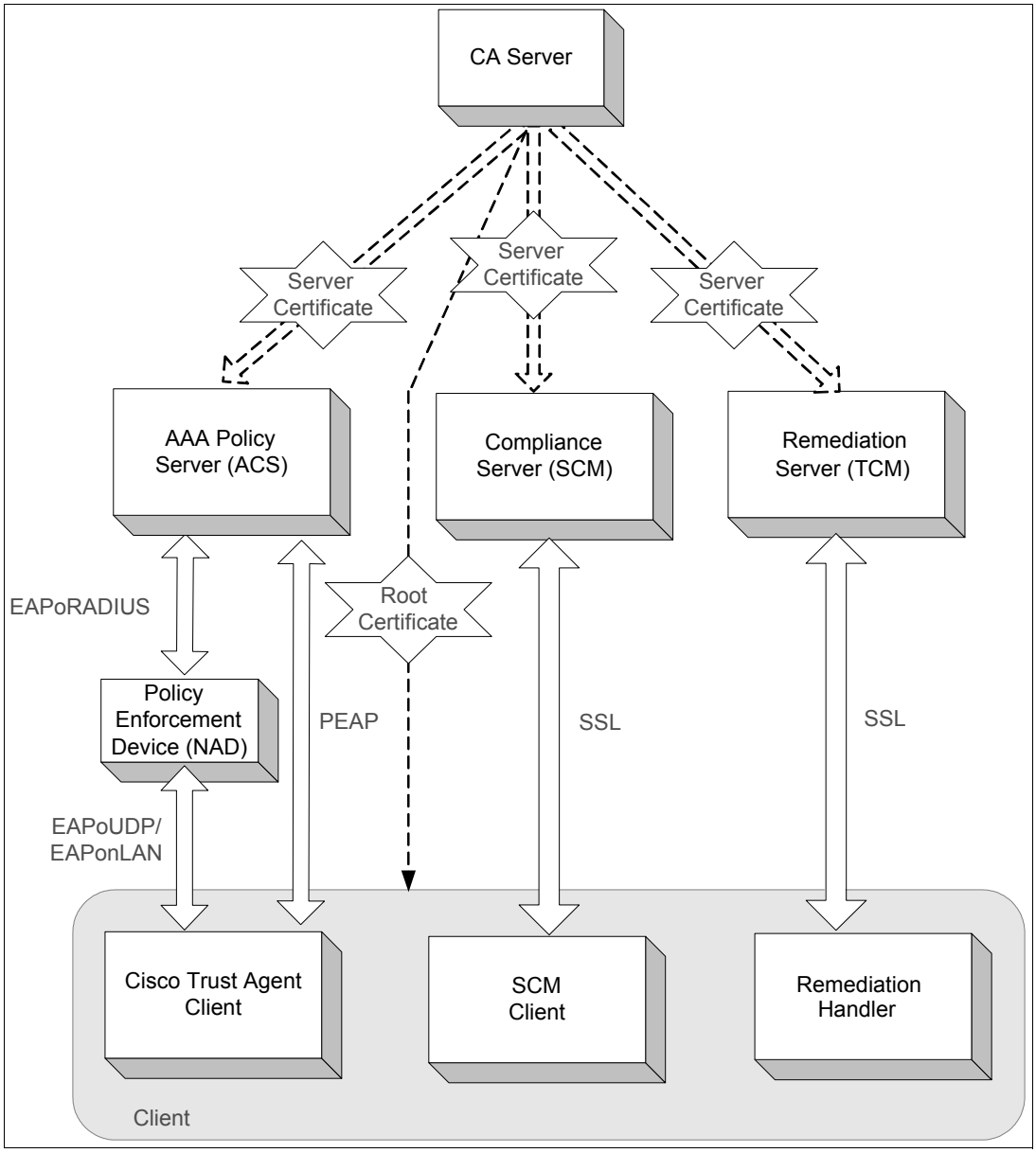


Figure 3-7 Secure communication between components

Downloaded from www.Manualslib.com manuals search engine

NAC communication

During communication of the Cisco Trust Agent client with the Cisco Secure ACS, a secure PEAP session is established with the network client and requests the network client security posture credentials.

Cisco Trust Agent uses certificates to establish a PEAP session with the ACS.

Security Compliance Manager communication

The Security Compliance Manager client communication with the Security Compliance Manager server is based on the server's self-signed SSL certificate and IP address or host name. Any other communication requests are denied. This assures that only the authorized Security Compliance Manager server can communicate with the particular client. The server presents its SSL certificate during the first communication with the client (first contact trust). This certificate is used to verify the server's unique identity and to encrypt all traffic within the Tivoli Security Compliance Manager environment.

Remediation communication

The communication between the remediation client and Tivoli Configuration Manager Web Gateway is based on HTTP, which means that if desired, an HTTPS session can be used to ensure confidentiality of the communications.

3.4 Component placement

Network security is an important consideration for most organizations. New systems and components that are deployed into the enterprise periodically due to business needs or security requirements must be deployed and should be consistent with existing security polices and architecture. This leads us into the discussion about where the various pieces of the IBM Integrated Security Solution for Cisco Networks can fit into in an enterprise network.

3.4.1 Security zones

As per IBM MASS (Method for Architecting Secure Solutions), networks can be divided into five major security zones.

- Uncontrolled zone/Internet, external networks
- Controlled zone/demilitarized zone (DMZ)
- Controlled zone/intranet
- Restricted zone/production network
- Restricted zone/management network

Downloaded from www.Manualslib.com manuals search engine

Figure 3-8 shows the security zones and their classifications. Organizations could have different topologies and have their own architecture and naming of zones depending on their security policy.

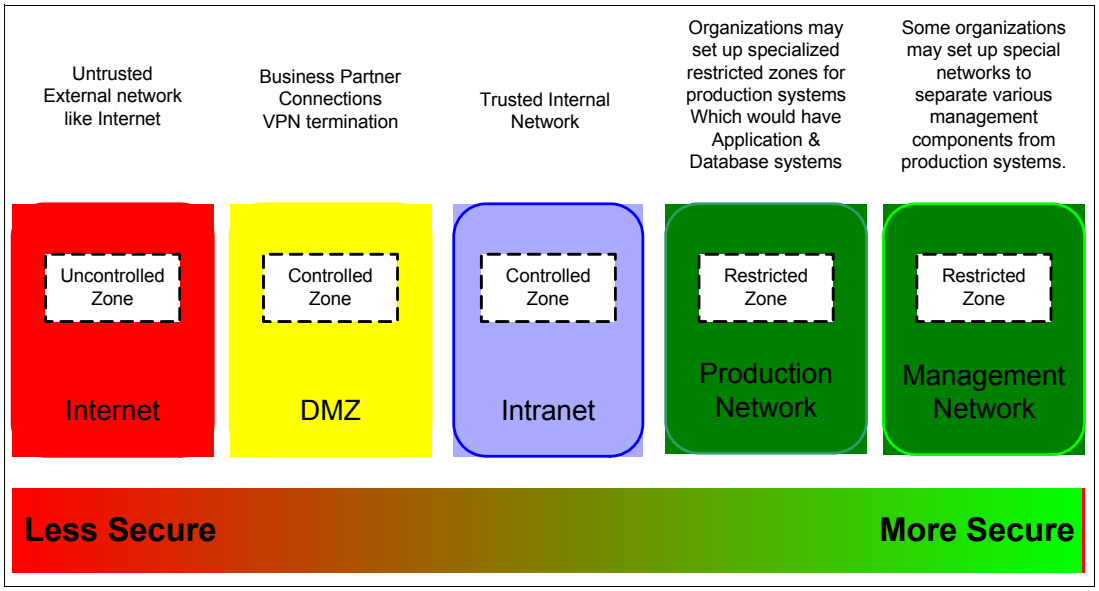


Figure 3-8 Security zones

For more about the MASS architecture methodology, refer to the IBM Redbook *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

Enterprise security has to meet many stringent requirements, one of them being compliance. Maintaining and enforcing client compliance can be a tedious process that consumes time and resources because:

- The number of clients can be large.
- Clients are physically dispersed and use different access methods to access enterprise resources.
- Not all clients accessing the network are owned by the enterprise (for example, partners and contractors).

The IBM Integrated Security Solution for Cisco Networks addresses network clients' compliance to policies that are centrally defined by the enterprise. The solution can enforce client compliance and help remediate compliance violations. Hence it is important to understand network clients, their access methods, and how this solution can effectively meet the end result of client compliance.

Network client machines represent the users of corporate resources. Clients access these resources using various access methods such as LAN, wireless, WAN, and Internet access. Clients using these access methods mostly enter the

Downloaded from www.Manualslib.com manuals search engine

corporate network through what are considered *external networks*, such as the DMZ and intranet zones.

Details of resources that are generally deployed in the various security zones, the possible access methods by which network clients access these enterprise resources, and the zones from which clients would access are discussed here and depicted in Figure 3-9. This discussion can help customers visualize the practical deployment scenarios of the IBM Integrated Security Solution for Cisco Networks in their organization.

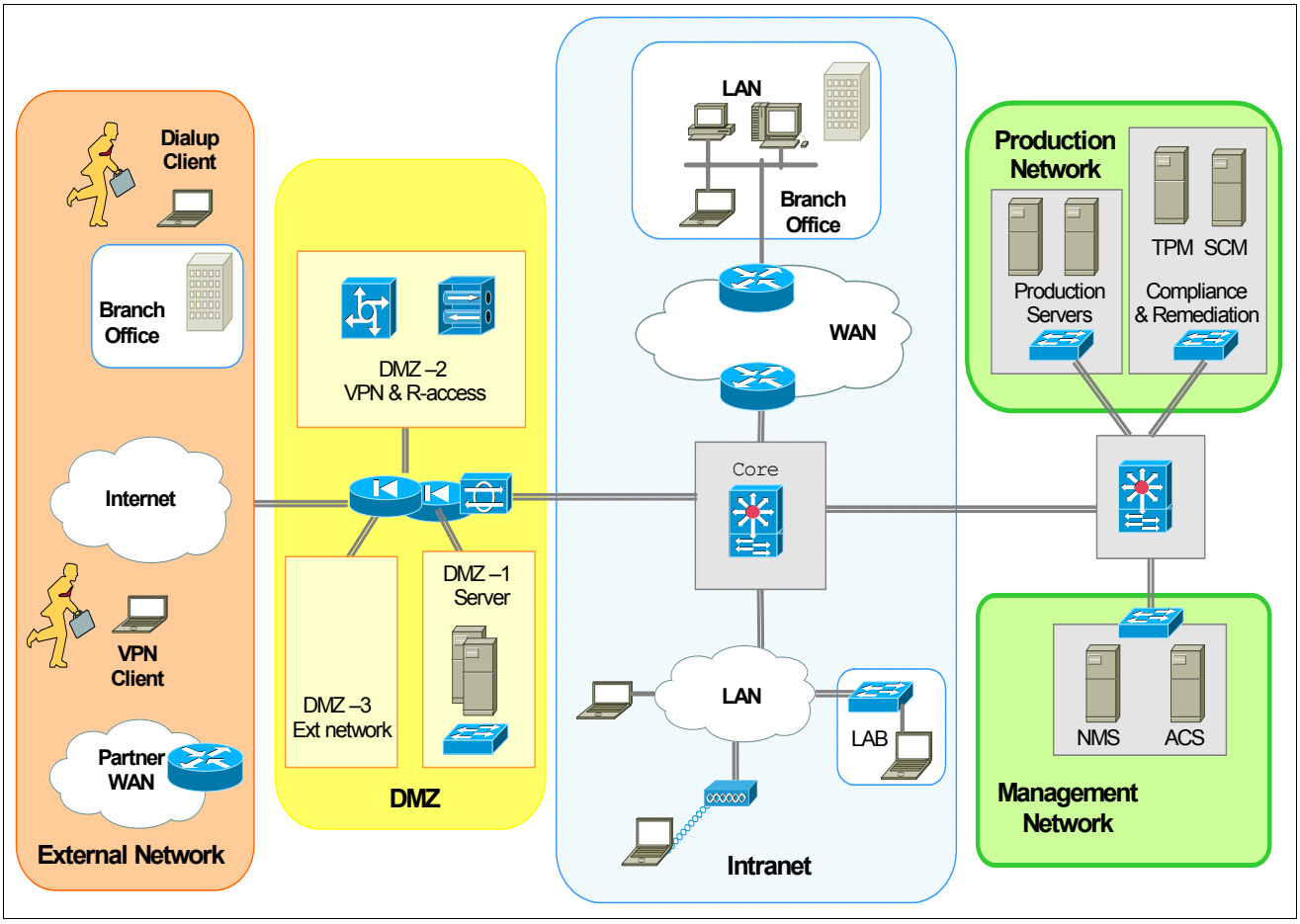


Figure 3-9 Client access to enterprise with zone details

Uncontrolled zone - Internet, external networks

The Internet has become a major business driver for many organizations, but it can be considered completely *uncontrolled*. Client machines use the Internet for the following means:

- Remote users can use the Internet as an access method and connect to enterprise resources using VPN technology from across the globe.

Downloaded from www.Manualslib.com manuals search engine

- Remote offices and branch offices can use the Internet as a primary method of access or for backup if the primary access method fails.
- Organizations can provide partners access over the Internet and exchange data over VPN.

Controlled zone - external network-facing DMZ

One *controlled*, semi-trusted network zone is called the DMZ. It provides a buffer zone between the Internet and internal networks. This zone can realize the following benefits:

- DMZ can terminate partner traffic or any other WAN traffic before it enters any restricted production zone.
- This zone terminates all dial-up users and VPN traffic.
- The Tivoli Configuration Manager Web Gateway is typically located in the DMZ.

Controlled zone - intranet

The intranet is the other *controlled* zone. Local client users on the LAN infrastructure and remote office users, using WAN-technologies to connect to various enterprise resources, are participants of this zone.

Restricted zone - production network

One or more network zones may be designated as *restricted* zones in systems to which access must be strictly controlled. These systems can be production servers and are typically application servers, database servers, and other servers that support business-critical functions. Direct access to these systems from uncontrolled networks should not be permitted. The Security Compliance Manager server, Security Compliance Manager proxy, and, optionally, the Configuration Manager Software Distribution server may be placed in the production network.

Restricted zone - management network

This zone contains network and enterprise management systems. The ACS can typically be part of the management zone.

Other networks

The network examples that we use do not necessarily include all possible scenarios. There are organizations that extensively segment functions into various subnetworks. However, in general, the principles discussed here may be translated easily into appropriate architectures for such environments.

Downloaded from www.Manualslib.com manuals search engine

3.4.2 Policy enforcement points

The IBM Integrated Security Solution for Cisco Networks employs the Cisco NAC solution to restrict access to users depending on the compliance level of the client. The NAC solution requires network access devices (NAD) to be deployed at various network points to enforce the policy. Some of the widely used network topologies and possible policy enforcement points are discussed here.

Branch office compliance

Most medium and large networks have regional and branch offices. Routers are usually deployed at both ends (for example, at the headquarters and the branch office). Hence there are two locations at which policy enforcement can be achieved at the branch router or at the headquarter router. In addition, if the branch office has a NAC-capable switch, the NAC policy enforcement can be implemented on the switch.

Branch egress enforcement

Regional and branch offices can have the policy enforcement point deployed at their location before they connect to the central data center at the branch routers itself (Figure 3-10).

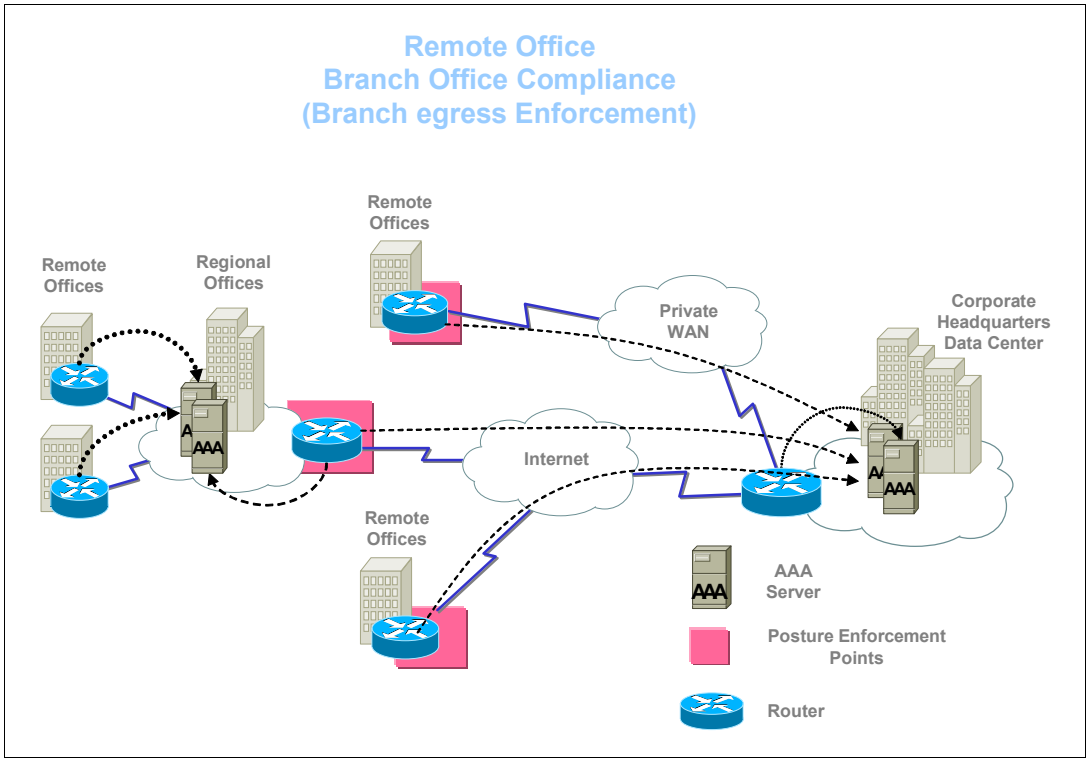


Figure 3-10 Branch egress enforcement

Downloaded from www.Manualslib.com manuals search engine

Advantages of this kind of deployment are:

- Policy enforcement load distribution across the various routers
- Protection against virus infection between branch offices if the network has a mesh topology

Factors that must be considered for branch egress enforcement are:

- Branch routers must support NAC
- Some additional administrative effort required during deployment

Campus internal enforcement

In this deployment option, the office policy compliance is enforced on all switches to which the users connect. Two modes of posture checking users exist within switches: 802.1x and EAP/UDP.

802.1x involves passing posture and, if desired, user authentication information in an EAP-based 802.1x frame. The response from ACS is a VLAN name or number associated with the posture state of the user, which would be healthy or quarantine.

EAP/UDP passes only posture information in an UDP datagram. ACS responds with a port-based ACL (PACL) that provides enforcement of users' healthy or quarantine state.

Note: At the time of this writing PACLs are not supported in an 802.1x NAC Framework on all Cisco devices. However, it is Cisco's stated intention to make this functionality available on all devices in the near future. Due to considerations that will affect the client software required on each endpoint, this book uses a reference architecture in which 802.1X is used for both authentication and admission control. This architecture delivers a valid network deployment even without PACLs and will be able to constrain traffic in a more granular fashion once PACLs are available.

The NAC Framework can work in IP Communications environments. For 802.1x environments, Cisco IP Phones must be used. For EAP/UDP environments, both Cisco and Non-Cisco IP Phones may be used.

Downloaded from www.Manualslib.com manuals search engine

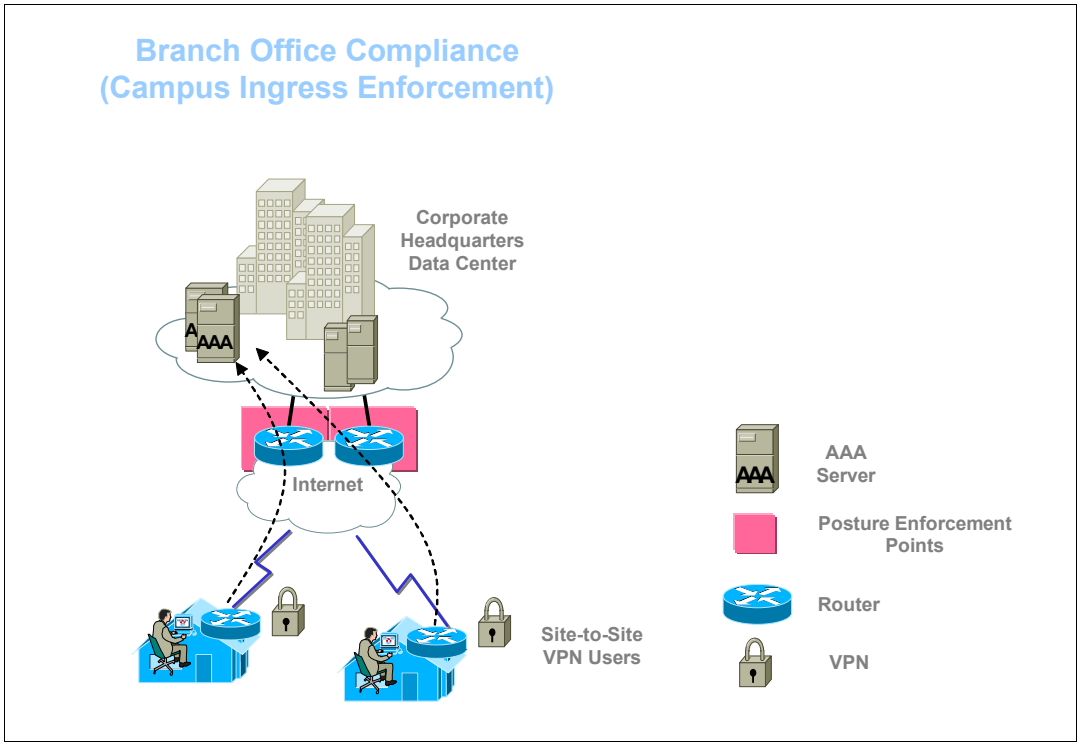


Figure 3-11 Campus ingress enforcement

Downloaded from www.Manualslib.com manuals search engine

Small Office Home Office compliance

Policy enforcement can be used to protect corporate networks from noncompliant and potentially infected small office and home office (SOHO) users, as shown in Figure 3-12. This will also be the practical deployment option for clients who are using Port Address Translation to access corporate resources.

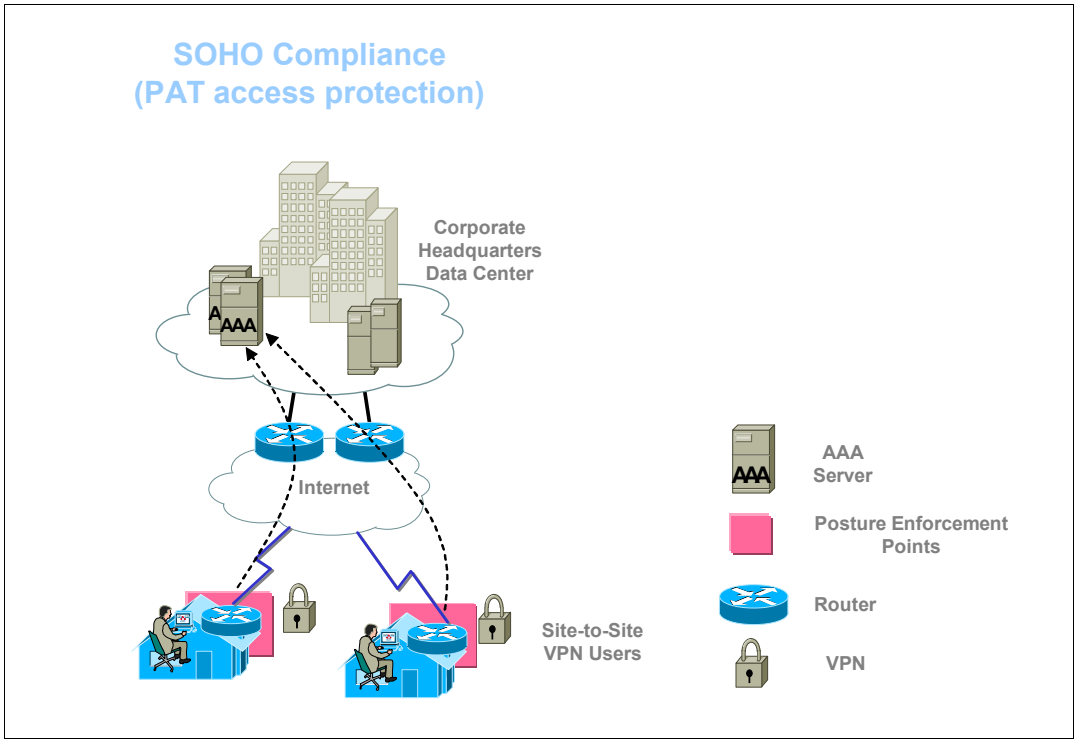


Figure 3-12 SOHO compliance

Downloaded from www.Manualslib.com manuals search engine

Extranet compliance

Organizations could have WAN connections to share information with partners. This would require partner systems connecting to the parent organization to comply with the policies laid down by the parent organization. The policy enforcement device can be deployed appropriately to ensure that these partner systems comply to the parent organization's policies (Figure 3-13).

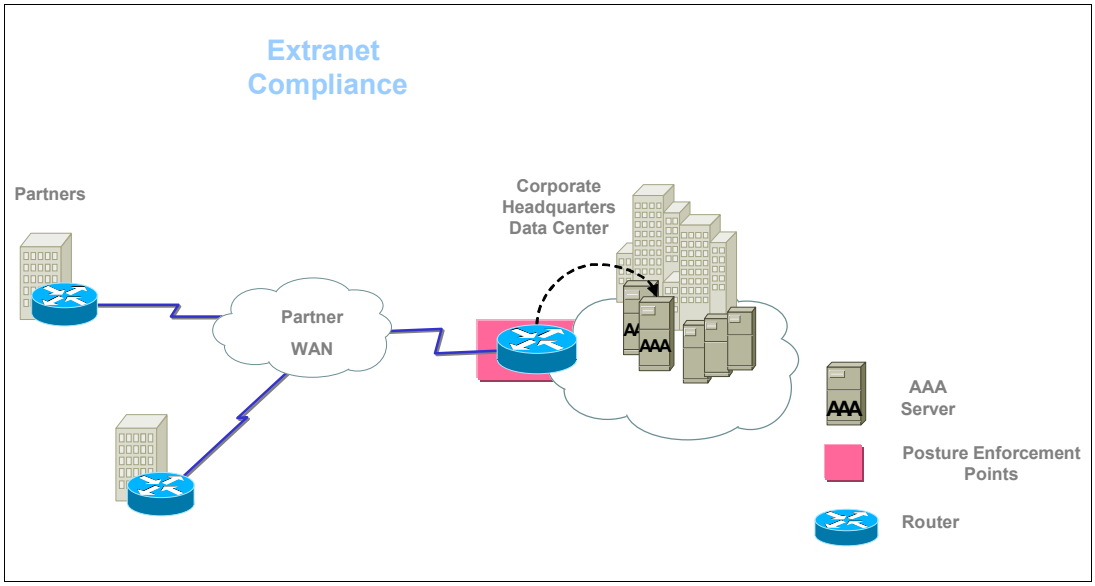


Figure 3-13 Extranet compliance

Downloaded from www.Manualslib.com manuals search engine

Lab compliance

Organizations prefer having lab networks to test systems before deployment of new solutions or equipment. Traffic from this zone to the primary network is restricted so that operations in the lab setup do not disrupt the production systems and networks. A policy enforcement at the connection between the production systems and lab setup can ensure that only systems that comply to the enterprise policy are allowed into the production network from a lab subnet. Figure 3-14 shows a lab policy enforcement scenario.

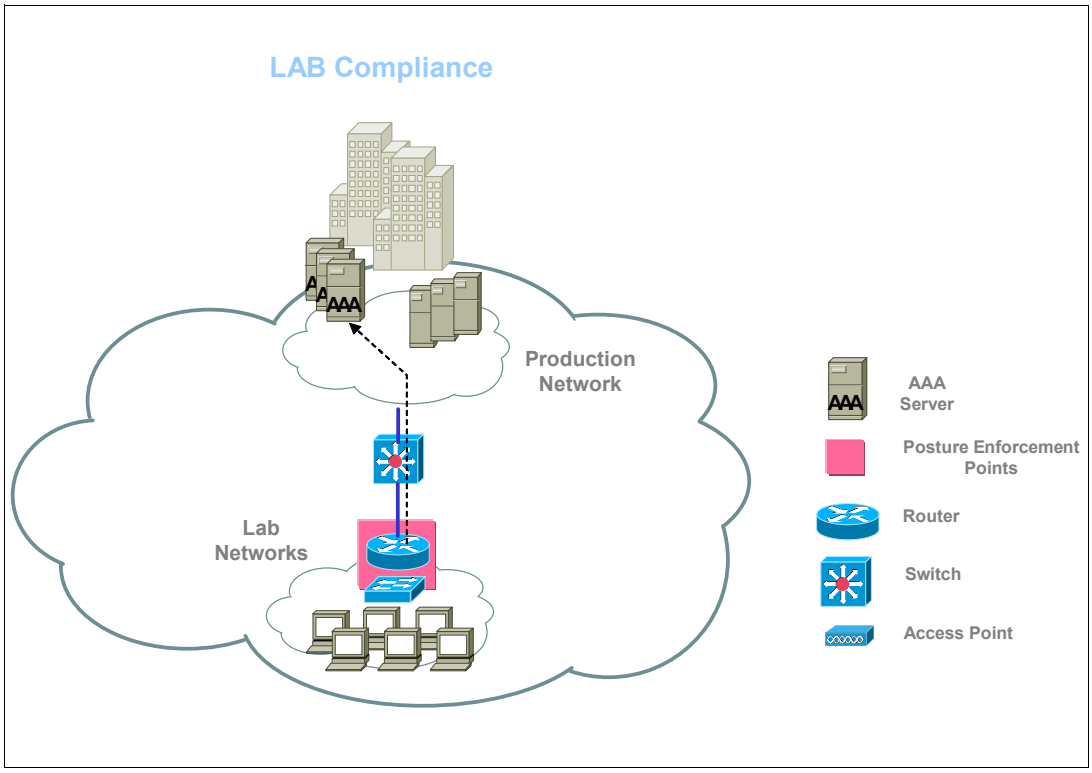


Figure 3-14 Lab compliance

Downloaded from www.Manualslib.com manuals search engine

Data Center protection

The Data Center is the site where organizations host business-critical systems that require maximum protection. Compliance can be checked for client systems before they are provided connections to the resources at the Data Center (Figure 3-15).

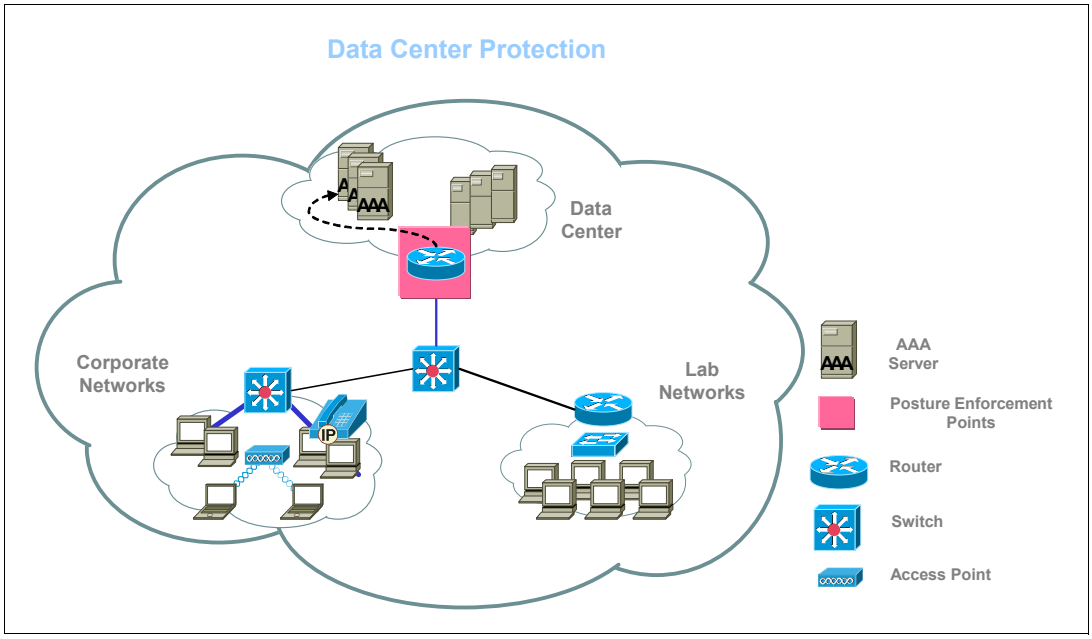


Figure 3-15 Data Center protection

Downloaded from www.Manualslib.com manuals search engine

Remote access protection

Remote access users use dial-up or VPN to connect to corporate resources. To enforce these users to comply to the corporate policies, a policy enforcement device may be deployed at the remote access entry points (Figure 3-16).

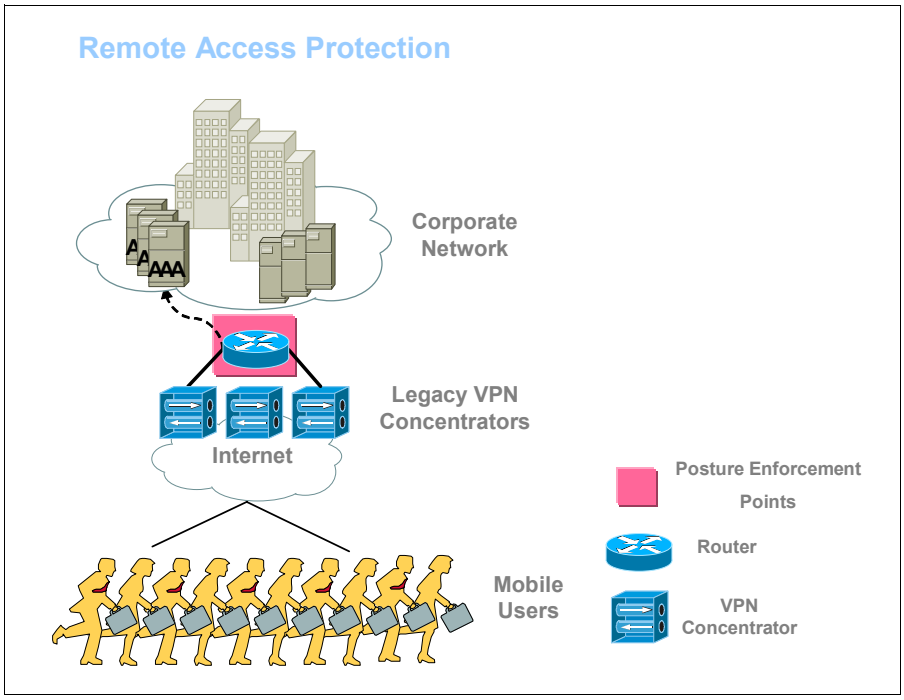


Figure 3-16 Remote access protection

The policy enforcement points can vary, depending on which section of the enterprise the organization would like to enforce compliance. The physical locations of posture enforcement points depend on the organization's network and security architecture.

3.5 Conclusion

The IBM Integrated Security Solution for Cisco Networks is an integration of products from IBM and Cisco. New components have been added to each of the individual product sets so they can work in unison. The components in this chapter have been described with integration being the prime objective. Some of the components can perform other functions not mentioned here. This chapter has dealt with the various logical and physical components that make up the IBM Integrated Security Solution for Cisco Networks. A logical data flow has been provided to show how the various components communicate and deliver the desired result of policy compliance validation and remediation.

Downloaded from www.Manualslib.com manuals search engine

Part 2

Customer environment

Part 2 discusses how the IBM Integrated Security Solution for Cisco Networks might be used in customer situations.

We use a well-know customer scenario, the Armando Banking Brothers Corp. In our last encounter in the IBM Redbook *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450, they successfully deployed the Tivoli Security Compliance Manager solution for their distributed server environment.

This time they are extending the use of Security Compliance Manager and, with solutions from Cisco and IBM Tivoli, they want to implement compliance-based physical network access control.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

4

Armando Banking Brothers Corporation

This chapter provides an introduction to the overall structure of the Armando Banking Brothers Corporation (ABBC). This introduction includes a description of ABBC's business profile, their current IT architecture, and their medium-term business vision and objectives.

Note: All names and references for company, personnel, and other business institutions used in this chapter are fictional; any match with real entities is coincidental.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

4.1 Company profile

Armando Brothers Banking Corporation (ABBC) is a fictional financial institution that traces its roots back to the early days of industrialization. During a time of radical change and growing financing needs, the Armando brothers founded a bank situated in the pioneer town of Waterloo — now known as Austin, Texas. In the early years, ABBC helped many entrepreneurial pioneers finance their business ventures. In part due to their history of progressive management, as well as their diligent awareness of emerging technologies, ABBC developed an ability to rapidly expand and open branches throughout the state, the nation, and ultimately the world. As the 20th century drew to a close, ABBC was an early adopter of electronic banking technologies; they were among the first banks offering their customers online account access. Today ABBC is one of the dominant players in the highly competitive realm of worldwide finance.

ABBC is keenly aware that providing increased electronic access for its customers requires ever-increasing security measures to protect its electronic assets. Currently ABBC is leveraging the existing IBM product solutions of the IBM Tivoli Identity Manager and the IBM Tivoli Access Manager to manage and enforce its authentication and authorization policies. Like many companies, ABBC has found that traditional hacker attempts to gain unauthorized access are only part of the security threat factor. In today's environment network, worms, trojans, and viruses pose an equally tangible threat. ABBC is aware that more than 90% of security attacks exploit known security flaws for which a patch is available or a preventive measure is known. ABBC is further challenged by compliance legislation such as the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX), as are many companies. To assist with both threat mitigation and management of business policy compliance issues, ABBC has adopted the IBM Security Compliance Manager product.

The inclusion of the IBM Security Compliance Manager product enables ABBC to reap a quick return on investment by automating and centralizing security compliance monitoring. Previously ABBC limited the use of the IBM Security Compliance Manager product to their servers. In the current project, ABBC will extend the use of the IBM Security Compliance Manger product to its workstations. Following workstation client deployment, they will embark on the next logical step: integrating their existing IBM Security Compliance Manager infrastructure with the Cisco-sponsored Network Admission Control program.

ABBC decided also to enhance the scope of the project by employing Tivoli Configuration Manager software currently used by the operations department to provide the users with help in keeping their workstation compliant with the corporate security policy.

Downloaded from www.Manualslib.com manuals search engine

4.2 Current IT architecture

This section provides background information about the existing Armando Banking Brothers Company IT architecture, including the network infrastructure, security infrastructure, and the middleware/application infrastructure.

4.2.1 Network infrastructure

Next we describe the logical network components that make up the ABBC network (Figure 4-1). ABBC has developed the network and application security infrastructure in line with the IBM MASS security model. The network has the following major security zones:

- Uncontrolled zone/Internet, external networks
- Controlled zone/demilitarized zone (DMZ)
- Controlled/intranet
- Restricted/production network
- Restricted/management network

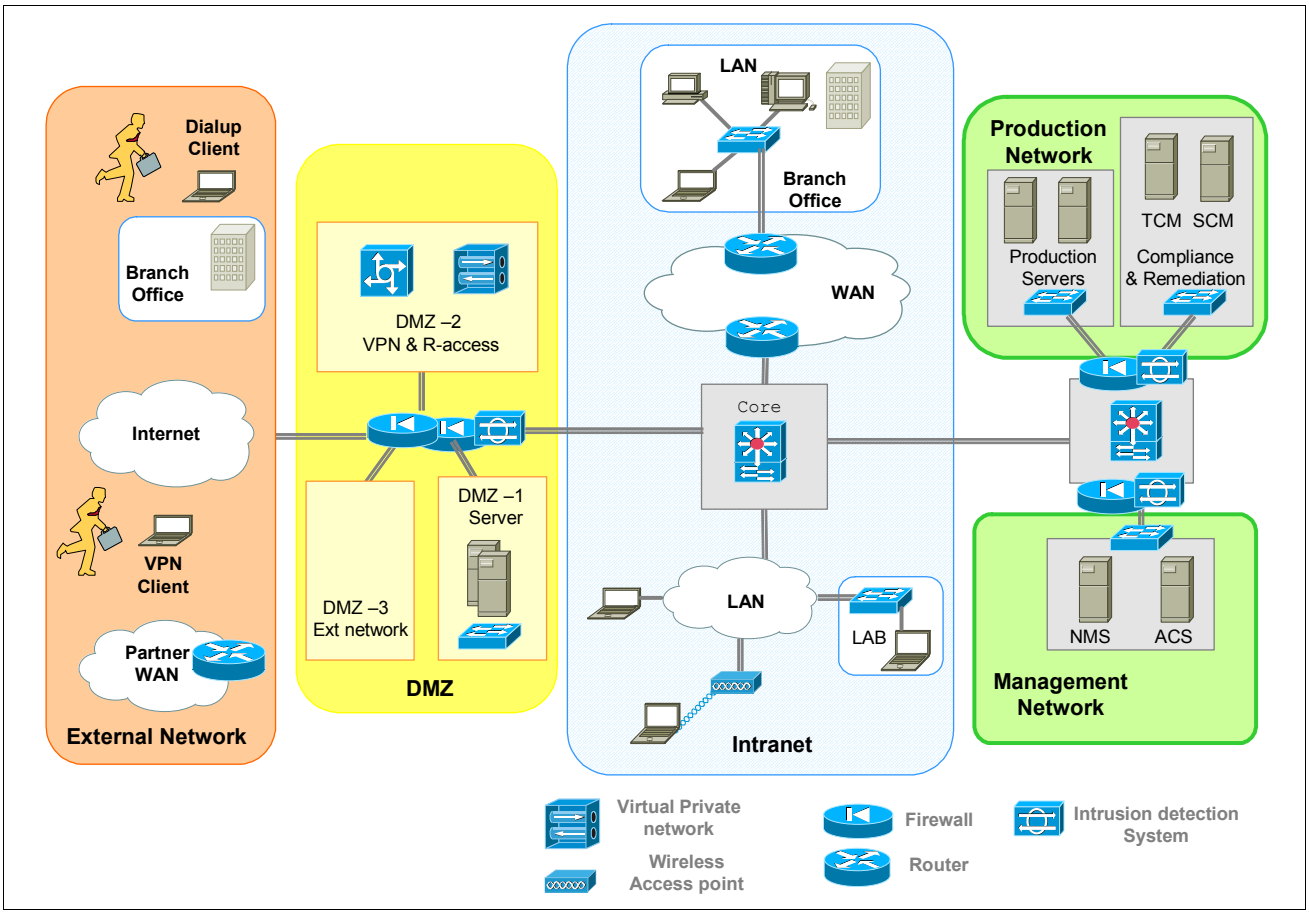


Figure 4-1 ABBC current network diagram

Downloaded from www.Manualslib.com manuals search engine

Uncontrolled zone - Internet

The Internet has become a pivotal component in the banking industry with its immense flexibility and business opportunities. But it has also become one of the preferred methods for spreading viruses and malicious code as well as providing easy access to many unprotected or weakly secured enterprise resources. Balancing the requirements and threats, ABBC has provided clients, employees, and partners with controlled access to its resources. Firewalls and intrusion detection and prevention systems have been deployed to provide adequate network perimeter security.

Controlled zone - DMZ

ABBC hosts Web access control servers and mail gateways in the DMZ. It is also a termination point for VPN users before they connect to the primary network.

Controlled intranet

Local employees connected through the LAN are part of this zone. ABBC is investing in wireless networks and VOIP technology for their users' improved access capability and flexibility. The corporate WAN also terminates in this zone. ABBC has a lab network where testing is done before any system is deployed in a production environment. The IBM Integrated Security Solution for Cisco Networks has been tested by ABBC. The test simulation is discussed briefly in 4.2.2, "IBM Integrated Security Solution for Cisco Networks lab" on page 80.

Production network

The server resources for the enterprise are deployed in the production network. With the IBM Integrated Security Solution for Cisco Networks, ABBC has deployed the compliance and remediation servers in this section of the network. The network management zone is a separate protected subnet. The segments of the production network are also given additional protection.

4.2.2 IBM Integrated Security Solution for Cisco Networks lab

Network Admission Control uses the network infrastructure to enforce security policy compliance on all devices seeking to access the network. NAC can be delivered in two ways: NAC Framework and NAC Appliance.

NAC Framework

NAC Framework is an architecture-based approach that provides comprehensive control by assessing all endpoints across all access methods, including LAN, wireless connectivity, remote access, and WAN. It can be deployed as NAC L2 IP, NAC L2 802.1x, or NAC L3 IP. It utilizes Cisco routers, switches, VPN Concentrators, and Adaptive Security Appliances. Cisco Secure ACS is an integral component of NAC Framework.

Downloaded from www.Manualslib.com manuals search engine

Figure 4-2 is representative of the ITSO Lab Environment used for L2Dot1x NAC deployment.

VLAN-11 Healthy Sales VLAN in the Core network. This VLAN hosts those users that have been authenticated by IEEE 802.1x as members of the Sales Group and have been posture validated as Healthy.

VLAN-12 Healthy Engineering VLAN in the Core network. This VLAN hosts those users that have been authenticated by IEEE 802.1x as members of the Engineering Group and have been posture validated as HealthyII.

VLAN-13 Quarantine Sales VLAN in the Core network. This VLAN hosts those users that have been authenticated by IEEE 802.1x as members of the Sales Group, but are not compliant.

VLAN-14 Quarantine Engineering VLAN in the Core network. This VLAN hosts those users hat have been authenticated by IEEE 802.1x as members of the Engineering Group, but are not compliant.

VLAN-9 This VLAN hosts the Cisco Secure ACS and the Tivoli Security Compliance Manager.

VLAN-104 This VLAN hosts the Tivoli Configuration Manager.

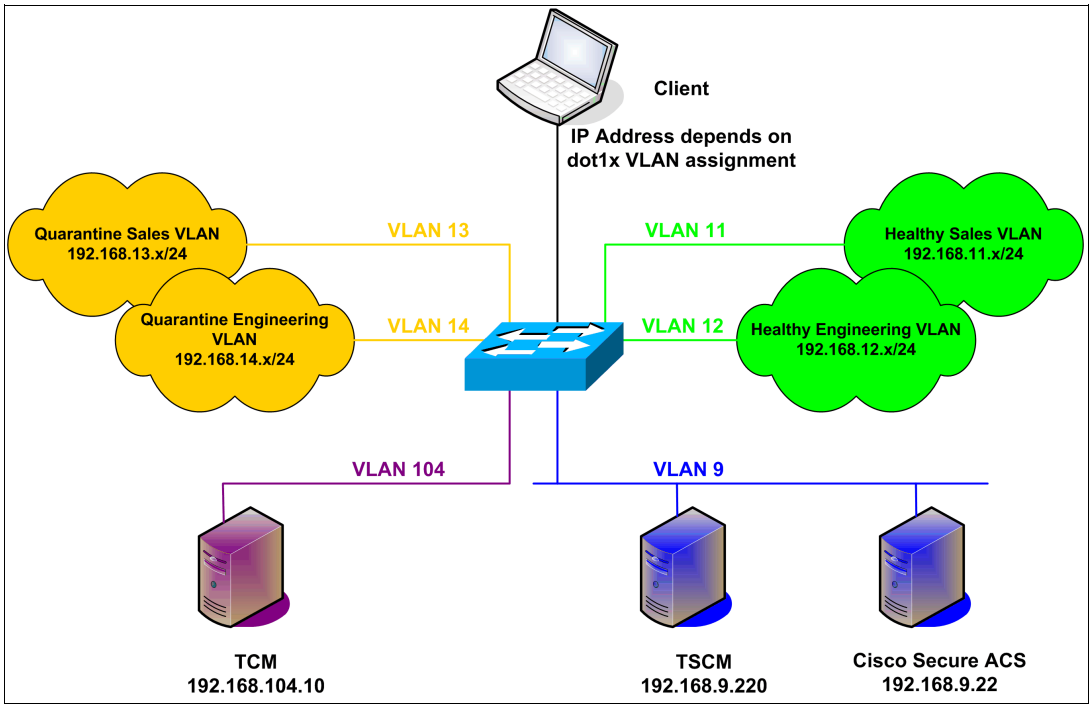


Figure 4-2 Armando Banking Brothers network environment for NAC Framework

From a Network Admission Control perspective, the user is prompted for his IEEE 802.1x credentials when he connects to the access switch. Upon supplying

Downloaded from www.Manualslib.com manuals search engine

his credentials, the Cisco Secure ACS checks its local user database and assigns the user to the respective group. The user is then mapped to the Healthy or Quarantine VLAN of that group, depending on the state of posture compliance provided by the CTA on the user's machine. All access to the network is based on access control lists (ACLs) bound to the Layer 3 Switched Virtual Interfaces (SVIs) on the switch, which in this example is also the access switch.

NAC Appliance

NAC Appliance is based on the Cisco Clean Access products. It comprises a Clean Access Manager (CAM), a Clean Access Server (CAS), and a Clean Access Agent (CAA). It is not based on an architecture approach, and can provide NAC functionality on non-Cisco based networks. NAC Appliance can be deployed in a variety of ways. In this example, it has been deployed as a *virtual out-of-band* gateway.

Downloaded from www.Manualslib.com manuals search engine

Figure 4-3 on page 84 is representative of the ITSO Lab environment used for NAC Appliance deployment.

VLAN 20 This is the Access VLAN for a Healthy user. All DHCP addresses are provided from VLAN 20, regardless of whether a user is compliant or noncompliant.

VLAN 120 This is the authentication VLAN. If a user is classified as noncompliant by the CAM, that user's switchport has its VLAN membership changed from VLAN 20 to VLAN 120. This is done by the CAM sending the relevant configuration commands to the switch using SNMP. Once the user is compliant, the CAM will again change the user's switchport VLAN membership, this time from 120 back to 20.

VLAN 9 This is the VLAN on the Core network where the CAM resides.

VLAN 10 This is the VLAN where the CAS sits. Note that both the untrusted and trusted interfaces of the CAS have the same IP address. This is a management IP address, and only the trusted interface is used for management sessions. VLAN 10 is on the VLAN allowed trunk list for the trusted interface only.

VLAN 998 This is the Native VLAN for the untrusted interface of the CAS.

VLAN 999 This is the Native VLAN for the trusted interface of the CAS.

Downloaded from www.Manualslib.com manuals search engine

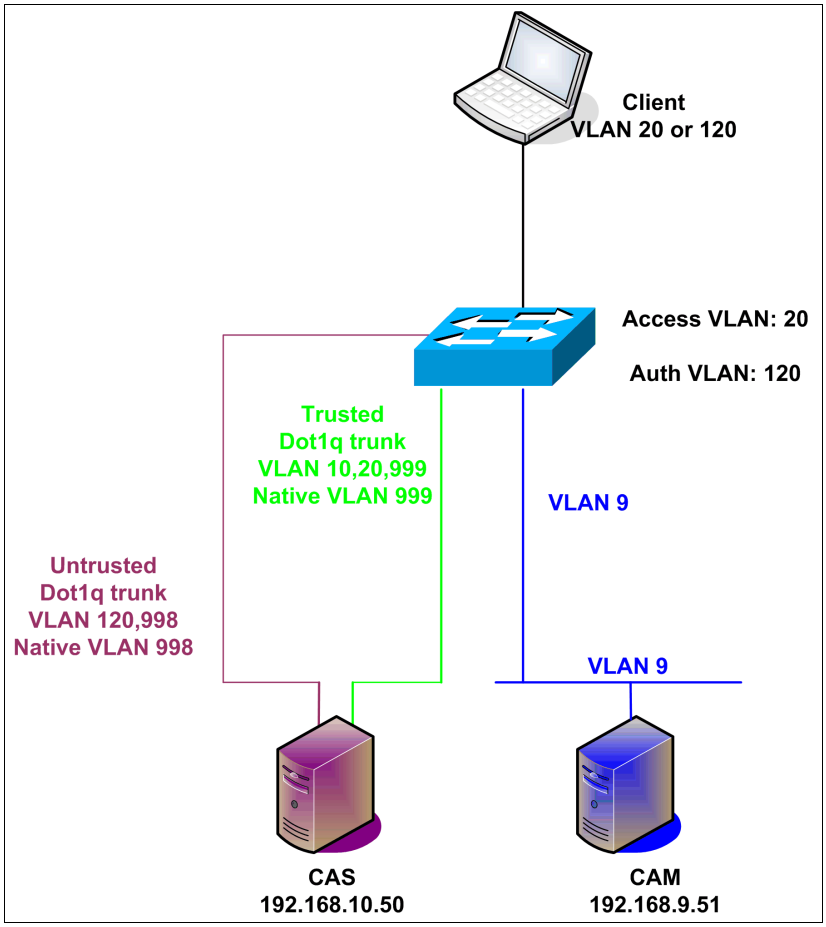


Figure 4-3 Armando Banking Brothers network environment for NAC Appliance

When a user connects to the network controlled by NAC Appliance, the CAM is advised of a linkup notification sent by the user's switch. The CAM checks its certified user list. If the MAC address is already present on the CAM as a certified user, and the credentials supplied at login are authenticated by the CAM, the user will be granted access to the network on their Access VLAN, which in this case is VLAN 20. If the MAC address is not present, or the credentials supplied are incorrect, the CAM will send an SNMP-write string to the user's switch, changing the switchport membership from VLAN 20 to VLAN 120. The user's IP address will remain the same, but he will be forced to go through the CAS. The CAS checks policy compliance and remediation. Once the CAS advises the CAM that the client is compliant, the CAM sends another SNMP-write to the user's switch, changing the switch membership from VLAN 120 back to VLAN 20. The user, now compliant, has access to the core network, bypassing the CAS.

Downloaded from www.Manualslib.com manuals search engine

4.2.3 Application security infrastructure

General management and the IT department are aware of the need for a solid basis to implement their future goals. The current environment with multiple systems is complex; the introduction of IBM Tivoli Access Manager for e-business in a previous project deployment provided a centralized, solid, and easy-to-manage security architecture to help control access to ABBC's Web-based assets and protect them from attacks.

Consistent with the ABBC commitment to proactively create a business environment in which continuous and sustained security control improvements are achieved, the introduction of IBM Security Compliance Manager for the ABBC server infrastructure provided a means to help establish effective audit readiness and compliance of their critical resources.

Downloaded from www.Manualslib.com manuals search engine

The diagram in Figure 4-4 provides a high-level graphical overview of the existing ABBC security infrastructure. We see that ABBC is using the IBM Tivoli Access Manager best-practice deployment methodology by incorporating dual multiple firewalls to secure the core network from external and internal users.

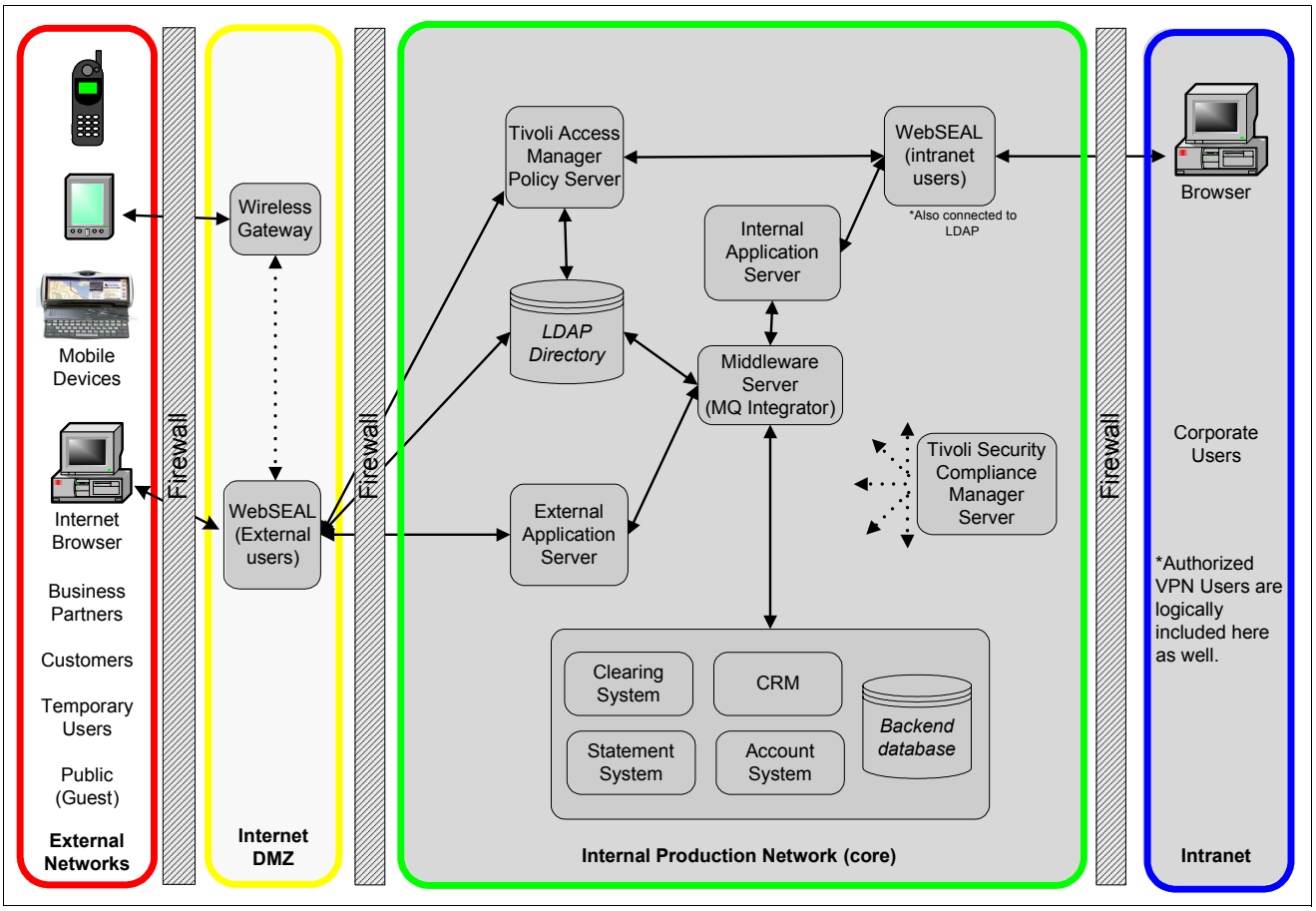


Figure 4-4 Armando Banking Brothers Company security and middlware infrastructure

Also note that in this diagram no distinction is made between the *type* of Internet users; in other words, local wired and wireless workstations, authorized remote access VPN sessions, and branch office connections are all considered part of the intranet and must pass through the internal firewall to access the secured applications.

We also see the Security Compliance Manager server in the core network.

4.2.4 Middleware and application infrastructure

In addition to illustrating the existing security infrastructure, Figure 4-4 provides a bit of data about the ABBC middleware and application infrastructure. Noting the *external application server,* we must understand that this one block represents a

Downloaded from www.Manualslib.com manuals search engine

cluster of IBM HTTP servers and WebSphere® Application Servers providing Internet banking and other services to external users. Similarly, the *internal application server* block represents multiple servers providing application support for internal users.

4.3 Corporate business vision and objectives

The Armando Banking Brothers Corporation (ABBC) has already made a significant investment toward securing their network infrastructure. Through the combination of forward thinking by ABBC management and technology from IBM, ABBC has been able to provide high availability of online banking services to its customers while minimizing the effects of nefarious network and application attacks.

ABBC is well aware that securing the network from external threats is only part of the story. Their mid-term vision is the monitoring, management, and enforcement of security policy compliance of its owned workstations used to access the corporate network, through local connections as well as via remote VPN technology. As a first step, ABBC deployed the IBM Security Compliance Manager solution to all of its server systems; this deployment provided monitoring and management of security compliance postures. Next, ABBC plans to extend the IBM Security Compliance Manager down to the workstation level, followed by the enforcement of security compliance postures through integration with Network Admission Control–enabled network hardware.

4.3.1 Project layout and implementation phases

In any deployment or introduction of new technology, it is important to know the goals and to properly set the expectation. Likewise there must be a way to measure project status. In this section, we describe the major steps that we cover in the banking scenario.

Defining the main security goals for the implementation, we shall assume:

- Business and security enhancements: As part of the implementation strategy, we present the additional business objectives and the security compliance–based Network Admission Control benefits that each new step adds.
- Pervasive security: The design principle includes making security part of the environment without disrupting services or user experience. As this is a major operational shift, the introduction of Network Admission Control technology will *not* be transparent to the end user. Therefore, the security goal is to provide high-quality security without unneccessarily inconveniencing users.

Downloaded from www.Manualslib.com manuals search engine

In the practice of IT security, it is possible to design an extremely secure, hardened system. However, this apex of maximum security will likely incur a cost of reduced system usability. Likewise it is possible to create a very user friendly, highly accessible network, but at a cost of reduced security. The IT Security Administrator must strive to strike a balance between these extremes. The introduction of a Network Admission Control system is a new technology for most, if not all, companies today. Armando Banking Brothers is no exception.

To implement the whole solution, ABBC has to designate the project, which will consist of three teams, each of them responsible for implementing one of the three parts presented below:

- Compliance team primarily responsible for implementing the corporate security policy for desktops in Tivoli Security Compliance Manager. This team will maintain the security policy, run the compliance audits, and operate the Tivoli Security Compliance Manager server.
- Network team responsible for configuration and maintenance of the Network Admission Control components enforcing the compliance to the security policy for the workstations connected to the ABBC's corporate network. This team is also responsible for network design allowing the noncompliant workstation to access the resources necessary for remediation as well as for the guest network access required by partners and contractors.
- Operations team responsible for user workstation configuration and user support. Part of their job is to maintain compliance of the user's workstations. They will facilitate this process by operating the remediation server that is already in use at ABBC: IBM Tivoli Configuration Manager. Enhanced, automated remediation capability provides a way to minimize user frustration, rising help-desk costs, and loss of user productivity.

Project overview

Table 4-1 provides a high-level overview of the major ABBC project parts and project steps. Remember, ABBC is a hypothetical company. There are many more steps, substeps, and considerations in an actual deployment. IBM always recommends the procurement of qualified service consultants as well as utilization of the IBM Solution Assurance Review Process.

Table 4-1 High-level project overview

Action	Notes	Reference
Part I - Security compliance server		
Tivoli Security Compliance Manager setup.	Detailed steps for a Security Compliance Manager server installation.	6.1, "Tivoli Security Compliance Manager setup" on page 126

Downloaded from www.Manualslib.com manuals search engine

Action	Notes	Reference
Configure Security Compliance Manager posture policy.	Ample thought time must always be provided for determining proper policy for the business. In a true deployment, the proper forethought, establishment of process, and policy are major keys to success.	6.2, “Configuration of the compliance policies” on page 152
Install compliance client software.	This includes both the IBM client components and the Cisco Trust Agent software.	6.3.1, “Cisco Trust Agent” on page 190, and 6.3.2, “IBM Tivoli Security Compliance Manager client” on page 199
Part II - Networking infrastructure		
	NAC Framework	
	Configuring the Cisco Secure ACS for NAC L2 802.1x	Highlights all the steps to configure the Cisco Secure ACS server for a NAC Framework NAC L2 802.1x deployment	7.1.1, “Configuring the Cisco Secure ACS for NAC L2 802.1x” on page 214
	Configuring the Cisco Secure ACS for NAC L2/L3 IP	Highlights the configuration changes that need to be made to the ACS to deploy NAC L2/L3 IP instead of NAC L2 802.1x	7.1.2, “Configuring the Cisco Secure ACS for NAC L2/L3 IP” on page 283
	Configuring Cisco 3750 switch for NAC L2 802.1x	Switch configuration and verification for NAC L2 802.1x deployment	“Configuring Cisco 3750 switch for NAC L2 802.1x” on page 292
	Configuring Cisco 3750 switch for NAC L2 IP	Switch and router configuration and verification for NAC L2 IP deployments	“Configuring Cisco 3750 switch for NAC L2 IP” on page 295
	Configuring Cisco IOS Router for NAC L3 IP	Switch and router configuration and verification for NAC L3 IP deployments	“Configuring Cisco IOS Router for NAC L3 IP” on page 298
	NAC Appliance	

Downloaded from www.Manualslib.com manuals search engine

Action		Notes	Reference
	Installing the Clean Access Agent	Highlights the steps for installing the Clean Access Agent	7.2.1, “Installing CCA Agent” on page 304
	Configuring a CCA OOB VG server	Highlights all the steps to configure the CAM and CAS for a Out-Of-Band Virtual Gateway server deployment	7.2.2, “Configuring a CCA OOB VG server” on page 306
	Configuring Cisco 3750 switch for NAC Appliance	Switch configuration and verification for Clean Access OOB VG deployment	“Configuring Cisco 3750 switch for NAC Appliance” on page 352
Part III - Remediation server			
Install base Tivoli Configuration Manager.		This solution assumes usage of already existing Tivoli Configuration Manager server. Detailed steps required were not described in this book. For the installation and configuration instructions refer to the product documentation.	*IBM Tivoli Configuration Manager Version 4.2.3 Planning and Installation Guide*, GC23-4702-03
Install Tivoli Configuration Manager Web Gateway.		This describes the installation of the prerequisites and Tivoli Configuration Manager Web Gateway component on top of the base Tivoli Configuration Manager installation.	8.2.2, “Tivoli Configuration Manager” on page 359, and *IBM Tivoli Configuration Manager Version 4.2.3 Planning and Installation Guide*, GC23-4702-03
Install and configure remediation package Web server.		This section describes the setup of the WebSphere application named SoftwarePackageServer, which is the interface between remediation handler on the client and Tivoli Configuration Manager Web Gateway server.	8.2.4, “Installation of the Software Package Utilities” on page 394

Downloaded from www.Manualslib.com manuals search engine

Action	Notes	Reference
Define or create HTML pages for assistance with remediation process.	Maps the posture policy to meaningful information to inform the user why they have been marked noncompliant, as well as what steps they have to take to remediate.	8.3, “Creating remediation instructions for the users” on page 397
Configure remediation workflows.	Links the Security Compliance Manager policy to the remediation actions.	8.4, “Building the remediation workflows” on page 417

4.4 Conclusion

Armando Banking Brothers Corporation (ABBC) is a company with a long history of leading-edge technology adoption. ABBC is well aware of the rising threats of computer viruses, worms, and the exploitation of known system vulnerabilities for which preventive measures exist. ABBC previously installed several IBM Tivoli security products in order to provide secure, scalable identity and access management of their IT infrastructure. More recently, in the face of growing concerns over threats, compliance-related risk, and government regulations, ABBC installed the IBM Security Compliance Manager product and uses it to proactively monitor compliance of their servers.

As the next major undertaking, ABBC is extending the Security Compliance Manager coverage to include the workstation systems of their internal and mobile workforce. The deployment of the Security Compliance Manager client to the ABBC workstations, through integration with Cisco Systems componentry, enables ABBC to deploy a Network Admission Control system based on posture compliance status.

ABBC intends to build the solution out of three major parts. The first part includes the deployment of the Security Compliance infrastructure and establishment of baseline posture policies. The second part covers the deployment and configuration of the network components to limit the network access for the noncompliant workstations. Finally, the third part extends the solution to include automatic remediation reusing the already existing Software Distribution software.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

5

Solution design

In this chapter we describe the business objectives that drive the functional requirements of the technical solution.

As a best practice, it is typical in a production environment to deploy a new technology, such as compliance-based Network Admission Control, in phases, aiming first at the selected test locations or user groups and then extending the project to the whole network. In addition, in a real-world scenario it is always necessary to first test any new technology in a dedicated test and development network before deployment to the production environment. This document assumes that all such test lab practices are transparently in place, so we discuss only the fictional production environment.

There are essentially three parts of this deployment scenario. In this chapter we explore how the functional requirements drive our project design.

Part 1, “Architecture and design” on page 1, is dedicated to the Security Compliance infrastructure, including server and client setup as well as policy creation and assignment. The detailed technical implementation of Part 1, “Architecture and design” on page 1, is described in Chapter 6, “Compliance subsystem implementation” on page 125.

Part 2, “Customer environment” on page 75, primarily involves adding posture compliance-based Network Admission Control components (servers and enforcement points) to the existing infrastructure. The detailed technical

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

implementation of part two is described in Chapter 7, “Network enforcement subsystem implementation” on page 213.

Part 3, “Appendixes” on page 439, builds on this infrastructure and adds automatic remediation functionality. The detailed technical implementation of Part 3, “Appendixes” on page 439, is described in Chapter 8, “Remediation subsystem implementation” on page 355.

Downloaded from www.Manualslib.com manuals search engine

5.1 Business requirements

As described in Chapter 4, “Armando Banking Brothers Corporation” on page 77, Armando Banking Brothers Corporation (ABBC) is well vested in the IBM Tivoli Identity, Access, and Compliance management solutions. With the emergence of the Network Admission Control program, as sponsored by Cisco Systems, it is ABBC’s direction to introduce a Network Admission Control program based on workstation posture-compliance status information.

The CEO of ABBC emphasizes the following business requirements:

- ABBC has experienced loss of productivity caused by the introduction of viruses and worms, the spread of which must be stemmed by limiting production network access to systems that comply with the ABBC security policy, such as weekly full-system scans.
- ABBC wishes to implement identity-based networking services, using the IEEE 802.1x protocol in the LAN environment, to identify who can access what information in the network.
- ABBC requires a method to ensure that basic safeguards are employed at the workstation level, such as:
  - Password quality standards
  - Detection of unauthorized Windows services
- ABBC requires a method to protect the mobile users from being attacked or infected when working outside of the corporate network by ensuring that personal firewall software is installed and running all the time.
- Mobile (and work-at-home) worker remote access must be maintained; at the same time, increased controls must be put in place to reduce risks to the corporate infrastructure.
- The solution must include a way to remediate noncompliant systems.
- The solution must be built largely upon existing infrastructure to help keep costs at a minimum.
- ABBC requires a minimally intrusive method to institute and enforce emergency change procedures for the company security posture-policy. The utilized method must not heavily consume help desk and system administrator resources.
- ABBC requires a method to ensure that required software, updates, and hotfixes are automatically installed on all workstations.

Downloaded from www.Manualslib.com manuals search engine

5.2 Functional requirements

In this section, the business requirements are further examined in order to extract the functional requirements. In subsequent sections of this book, the functional requirements are further distilled down to the implementation details.

5.2.1 Security compliance requirements

As we further examine our security compliance-related business requirements, we find that the following pain points are the requirement drivers.

- Viruses and worms are becoming more sophisticated, both in their ability to propagate themselves and in causing major business disruptions.
- Only authorized workstations should be allowed onto the network.
- Users often change local workstation security settings and run unauthorized services, thereby making their workstation inherently less secure.
- The operational-level security policy is changing frequently, especially with the high number of security updates and hotfixes being released by the operating system vendor.

5.2.2 Network access control requirements

Examining network security related requirements we found that the following pain points are the requirement drivers:

- The mobile worker presents a challenge for IT staff because of a general lack of ability to ensure that company computer image and update polices are followed.
  - Mobile users often move back and forth from client-networks to the ABBC-network, thereby increasing the exposure risk.
  - Mobile and work-at-home personnel often access the corporate network from home-based networks shared with other family members, again increasing the exposure risk.
- Uniform security policies, no matter where a user tries to connect from.
- The traditional perimeter defense is no longer sufficient because the perimeter is very porous in today's business environment.
- Locating and isolating noncompliant systems consumes time and resources.

Downloaded from www.Manualslib.com manuals search engine

5.2.3 Remediation requirements

Examining the operational maintenance related requirements we found that the following pain points are the requirement drivers:

- Desktop security requirements became so complex that most of the non-technical end users cannot track the policy changes on their own.
- Increasing numbers of mobile users are outside of the scope of the desktop policy enforcement realized with Active Directory®.
- Installation of hotfixes, security updates, and network supplicant software must be strictly controlled due to change management process requirements.
- Enforcement of security policy without facilitating the remediation process results in productivity loss and an increased number of help desk calls.

Finally, one of the ABBC general functional requirements is *an ability to institute and enforce emergency change procedures for the company security posture policy*. The associated pain point is straightforward. Consider a scenario where a potential severity-one Windows vulnerability has become public and Microsoft has issued a hotfix for this vulnerability, which is of sufficient severity that the normal change procedure documented in 2.3.2, “Security policy life cycle management” on page 30, is not practical. However, while incorporating the emergency change procedure, maintaining employee productivity must also be considered, as ABBC must continue to do business and serve its customer base. In addition, the solution has to consider the bandwidth and resource limitations of the ABBC help desk staff and system administrators. The ABBC help desk cannot sustain a deluge of help requests from scores of users who are suddenly denied access for noncompliance. Combined with the ability to institute emergency posture-policy changes, remediation requirements also include the need to be able to push a critical system update, such as a severity-one hotfix. Fortunately, all of the requirements can be met by combining posture checks with network access enforcement and an automatic remediation facility.

5.2.4 Solution functional requirements

ABBC has well-defined security policies for their servers, as well as the existing infrastructure to measure and track compliance via the IBM Tivoli Security Compliance Manager product. However, ABBC lacks a technical method to check security compliance of the users’ workstations, which are known to contain a lot of the company’s sensitive data. Thus, as we examine the requirements, along with the pain points, we find that they can be condensed into three functional requirements.

The first functional requirement is to *centrally manage and track the workstation compliance status* for all the users’ workstations, both stationary and mobile. This

Downloaded from www.Manualslib.com manuals search engine

allows us to warn users if any noncompliance is found and explain the current desktop security policy requirement. This helps to keep users aware of the current security policy requirements and allow reporting on the compliance status of all of the workstations in the environment.

The second functional requirement is to *restrict network access for noncompliant workstations*. This limits or prevents the interruption of network operations caused by worms and other hostile software.

The third functional requirement is to *provide a means of facilitating automated remediation for eligible workstations*. While increasing the security level, the solution should not increase the operational costs of maintaining the workstation environment.

Utilizing the existing Tivoli Security Compliance Manager and Tivoli Configuration Manager software minimizes training and maintenance costs, thereby addressing the fiscal business requirement. Note that the Network Admission Control methodology is being extended only to workstations.

Downloaded from www.Manualslib.com manuals search engine

ABBC will institute posture-based network admission. Systems deemed in noncompliance will be quarantined and allowed to access only the remediation network. Figure 5-1 shows a conceptualized view of the functional requirements.

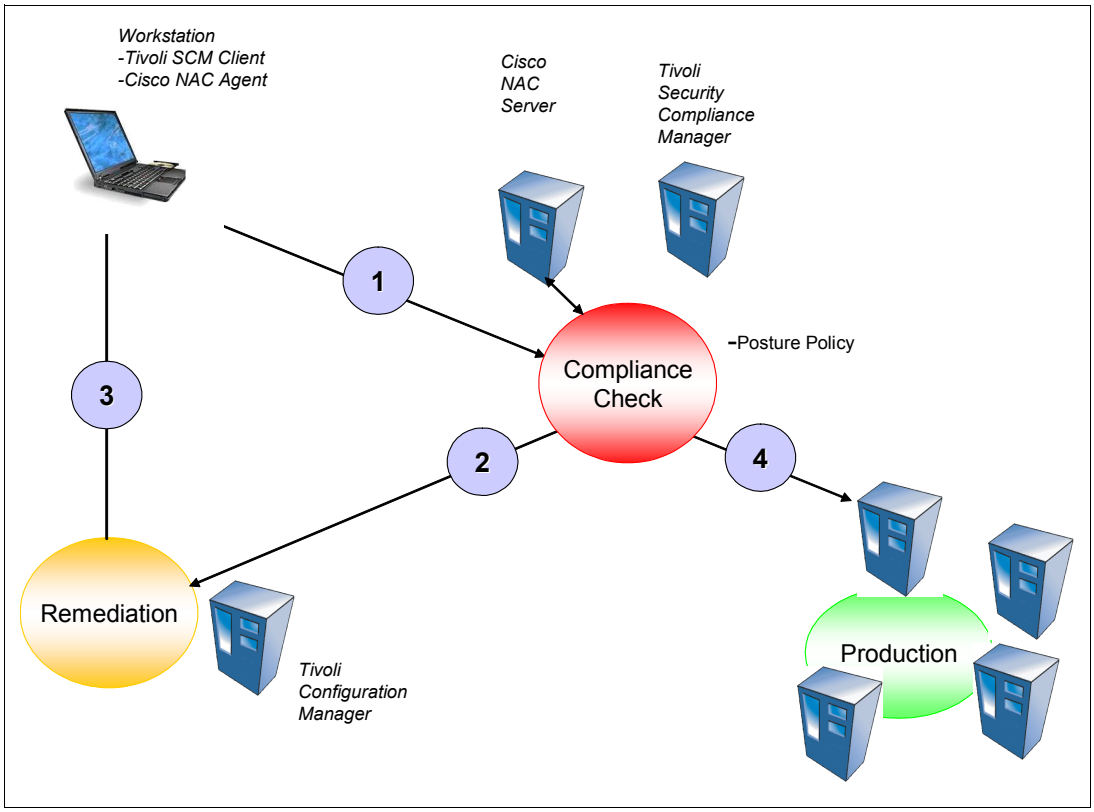


Figure 5-1 NAC solution conceptual functional requirements

The steps of the basic flow are:

1. The workstation, whether local or remote, attempts to access the ABBC network. IEEE802.1x credentials are supplied.
2. A *compliance check* is initiated by the Cisco Network Admission Control enabled device (for example, a router, switch, or Clean Access Server). This enforcement device requests the posture status from the client, then queries the Cisco NAC server (may be Cisco Secure Access Control Server or Clean Access Manager) policy to make an access decision. If the system meets the posture policy criteria, it is allowed access to the production network. For illustration purposes we assume that the system does not meet the criteria, and we continue through the flow.
3. Having failed the posture compliance check, the client workstation is denied access to the production network. The workstation is now considered to be in *quarantined* status and is allowed to access only a subset of the network (what we are calling the remediation network).

Downloaded from www.Manualslib.com manuals search engine

4. The Security Compliance Manager client is armed with a *remediation handler*. The remediation handler provides a method of displaying the compliance posture data to the end user. In addition to informing the user of the specific posture failures, the remediation handler can display additional, customizable information informing the user what the current security policy requirements are and what steps have to be taken and whom to contact for additional assistance with resolving the specific compliance violations. Finally, the remediation handler also provides a method for reinitiating the local security compliance scanning process.
5. When the workstation has completed the remediation process and is healthy again, it will be allowed access to the production network following the next periodic status query issued by the Cisco enforcement device.

Security compliance criteria

According to the published security policy for desktops, ABBC will institute the following compliance criteria for Network Admission Control checking:

1. Local workstation password quality must meet the following criteria:
   a. Password age must not be older than 90 days.
   b. Password minimum length must be eight characters.
2. The Windows Messenger service on user workstations must be disabled.
3. A system must have run a full virus scan during the past 7 days.
4. The antivirus software version must be correct (Symantec Antivirus Version 9.0.3.100).
5. The virus definition file must be up to date, meaning not older then September 29th, 2006.
6. The users' workstations have to run Windows XP Service Pack 2.
7. There must be specific Microsoft hotfixes (for example, we used KB896423 and KB893756) installed on the workstation.
8. The personal firewall software must be installed and running.
9. The Windows messenger service must not be allowed.

Remediation services

ABBC will deploy and configure the infrastructure to enforce network admission based on business policy. However, to minimize the impact on users' productivity the remediation methodology will utilize automated remediation processes.

It must be noted that the Network Admission Control (NAC) system is not intended to be a replacement for traditional workstation life cycle management. As documented in 2.3.2, "Security policy life cycle management" on page 30, we

Downloaded from www.Manualslib.com manuals search engine

recommend that a process be in place for the normal notification and distribution of required workstation updates and corporate policies; for all but the most extreme cases, the life cycle management process includes a grace period.

The deployment of the NAC, along with the IBM Integrated Solution for Cisco Networks, enables ABBC to *enforce* policy by blocking the network access of noncompliant systems after the expiration of this grace period. Figure 5-2 illustrates a client system in violation of the password quality check. Note that the remediation handler interface provides the user with a description of the violation and the steps necessary to resolve the issue. These may or may not include calling the remote remediation server in order to download appropriate software and execute the actions to get the workstation back to the compliant state.

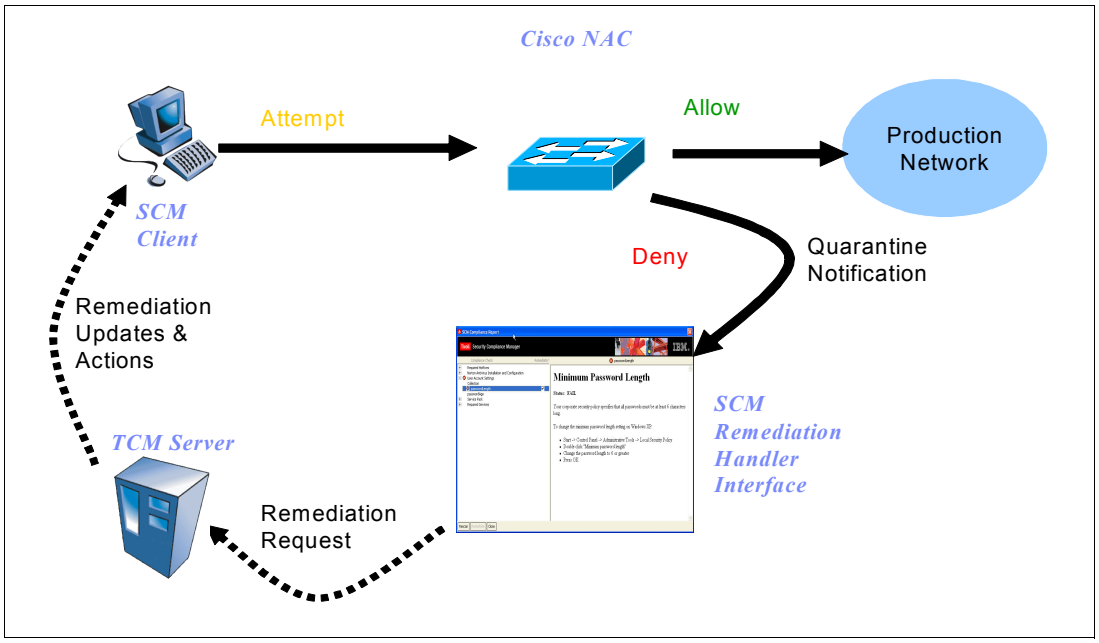


Figure 5-2 Remediation process

5.3 Implementation architecture

Network Admission Control (NAC) is not a single product; NAC is an industry-wide collaboration sponsored by Cisco Systems. As such, a NAC implementation requires a multivendor collection of physical and logical components.

As referenced in Figure 5-3 on page 102, the major Cisco components include a client-side Cisco Trust Agent, a Cisco Network Access Device (NAD) running a NAC-enabled version of Cisco's IOS, and a Cisco Secure Access Control Server (ACS) running Version 4.0 or later software. The major IBM components of the

Downloaded from www.Manualslib.com manuals search engine

integrated solution include the Security Compliance Manager client/server componentry and the Tivoli Configuration Manager remediation client/server code.

In this section we see how these components map to the implementation architecture.

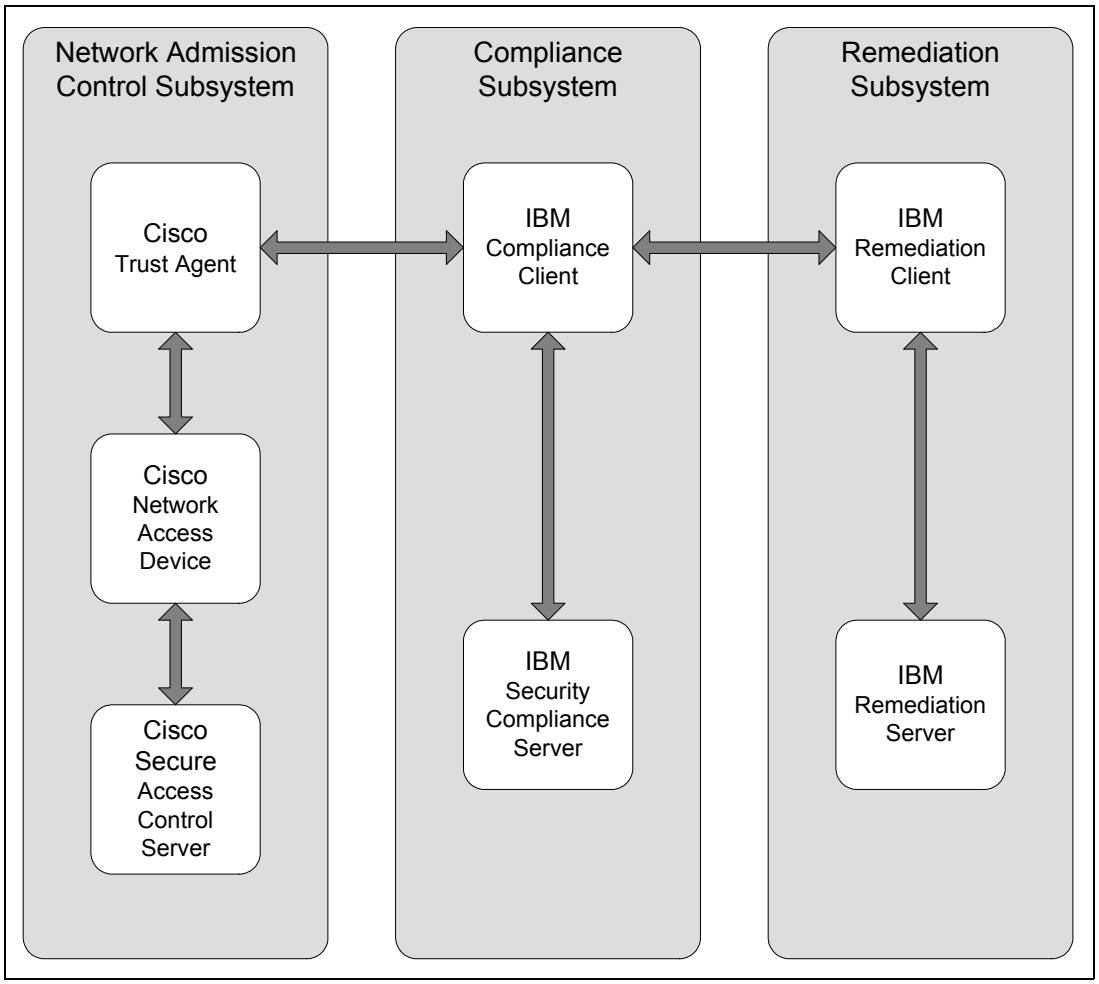


Figure 5-3 Component subsystems - total solution

5.3.1 Logical components

For the purposes and scope of this book, we operate under the premise that ABBC has the software distribution server subsystem based on the Tivoli Configuration Manager installed and configured. For detailed information about basic implementation of IBM Tivoli Configuration Manager refer to the product documentation *IBM Tivoli Configuration Manager Version 4.2.3 Planning and Installation Guide*, GC23-4702-03. Here we focus on extending the infrastructure

Downloaded from www.Manualslib.com manuals search engine

with the Web Gateway component to allow for automated remediation at the workstation level without need of having Tivoli Framework endpoint installed.

Again referencing Figure 5-3 on page 102, note that the total solution is comprised of three major subsystems: the compliance subsystem, the Network Admission Control subsystem, and the remediation subsystem. The implementation of these subsystems is described in the following three chapters.

In logical terms, we can span both the Network Admission Control subsystem and the compliance subsystem into a logical *network admission policy.* This collective network admission policy is comprised of the establishment and enforcement of compliance criteria.

Establishing compliance criteria

In this section we describe the process of establishing the compliance criteria based on the security policy for desktops described in 5.2.1, “Security compliance requirements” on page 96.

Configuring the compliance server

Let us create the compliance criteria, the policy, that is used to evaluate the client posture. Chapter 6, “Compliance subsystem implementation” on page 125, describes the detailed flow of the overall installation and configuration, including the assignment of the policy to the client groups. Additionally, administrative Security Compliance Manager information, such as importing and modifying policies, can be found in the *Tivoli Security Compliance Manager Version 5.1: Administration Guide*, SC32-1594. Our focus here is to show how to manage the policy versioning needed for policy life cycle management.

The IISSCN_TCM_v2.00_WinXP.pol policy bundle, which is available from the IBM Tivoli Security Compliance Manager 5.1 Utilities Web page (see “Online resources” on page 484), is used as our initial reference policy. This policy bundle contains the posture collectors that are used to make client-side compliance decisions. This policy is imported into the IBM Security Compliance Manager environment and modified to meet ABBC’s functional requirements.

Note: This solution is still being developed, so it is likely that the specific version of the referenced posture policy, IISSCN_TCM_v2.00_WinXP.pol, may not be publicly available by the time you read this book. However, we expect that the general contents of the default posture policy will be fairly consistent. Thus, the procedures for setting up policies as outlined in this book most likely can be followed using the policies that IBM has available.

Downloaded from www.Manualslib.com manuals search engine

Establishing the policy collector parameters

At this point, we have to establish the posture policy version because this has a direct bearing on how the network access control permissions will be set. Figure 5-4 shows a logical view of the Tivoli Security Compliance Manager client components.

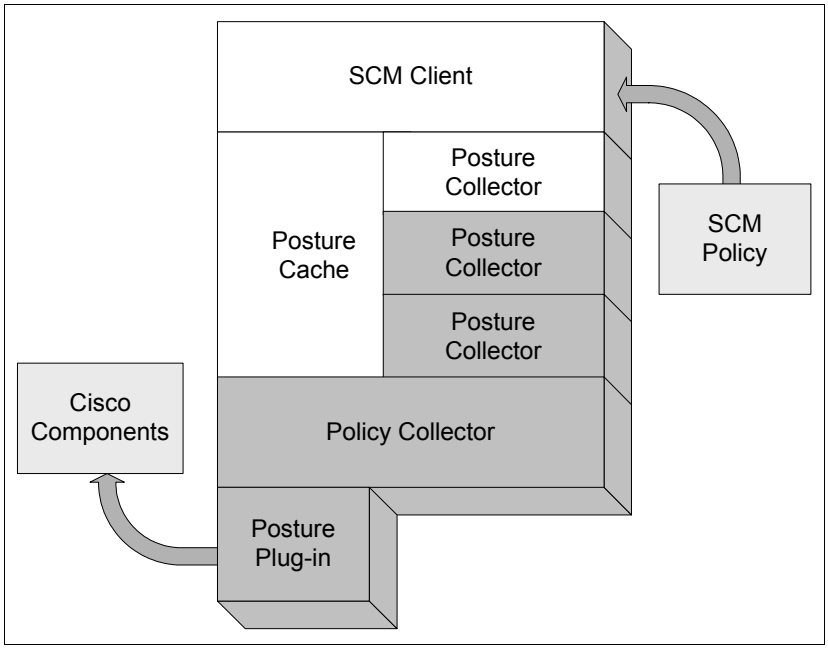


Figure 5-4 Tivoli Security Compliance Manager client components

The *policy collector* gathers data from the posture collectors and passes it to the posture plug-in, after which it is forwarded to the Cisco components for the access decision. See “Compliance client” on page 48 for more about these client components.

Tip: Other terms used to describe the unique nature of the policy collector include *management collector*, *meta-collector*, and *hypervisor*.

Downloaded from www.Manualslib.com manuals search engine

Although the policy collector *appears* to be at a peer level with the posture collectors in Figure 5-5, it is actually a hierarchical relationship, as shown in Figure 5-4 on page 104.

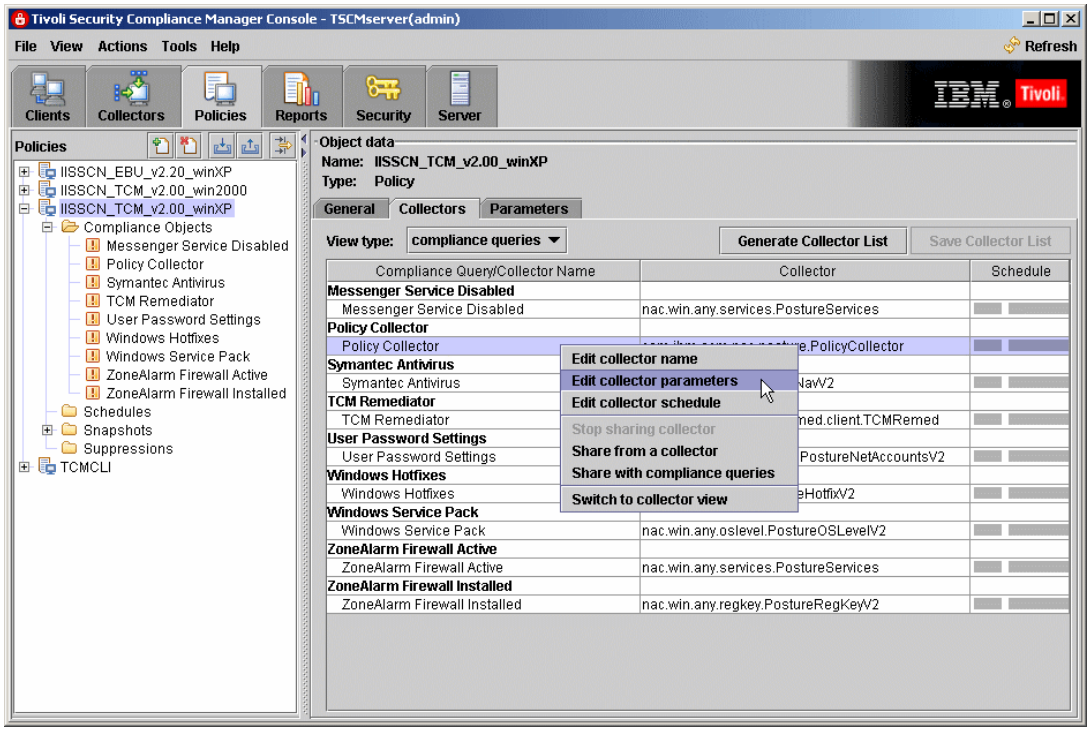


Figure 5-5 Security Compliance Manager policy collector - edit collector parameters

The Tivoli Security Compliance Manager policy collector parameters are set exactly the same way the posture policies are set. Refer to Chapter 6, “Compliance subsystem implementation” on page 125, for a detailed description of the procedure.

Downloaded from www.Manualslib.com manuals search engine

There are several parameters of interest:

- The *POLICY_VERSION* parameter (Figure 5-6) establishes the version level of the policy. This field is simply a string value. The company version control process is strictly a manual one. During the network admission check, this version information is used to ensure that the client has an acceptable version of the compliance policy. (More on this in the next section.)

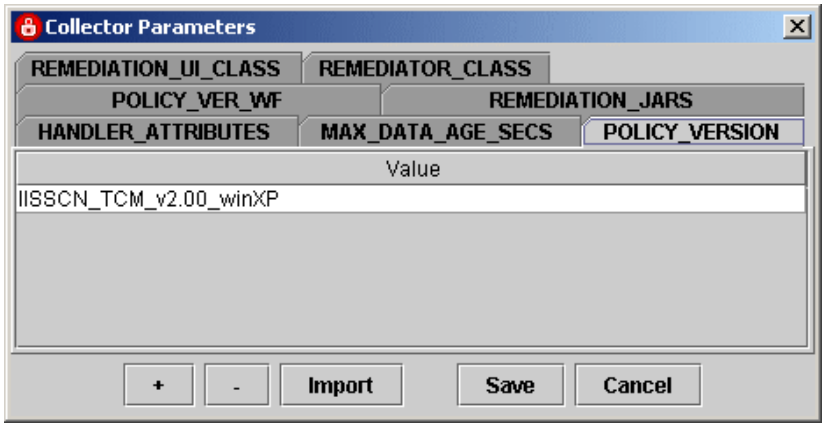


Figure 5-6 Setting the policy version

- The MAX_DATA_AGE_SECS parameter (Figure 5-7) establishes the maximum data age for the posture cache data: When the workstation is challenged by the network for posture status it returns the data from its cache if the data is more recent than the maximum data age parameter. Otherwise the posture collectors are triggered, the posture cache is refreshed, and the posture data is returned to the network.

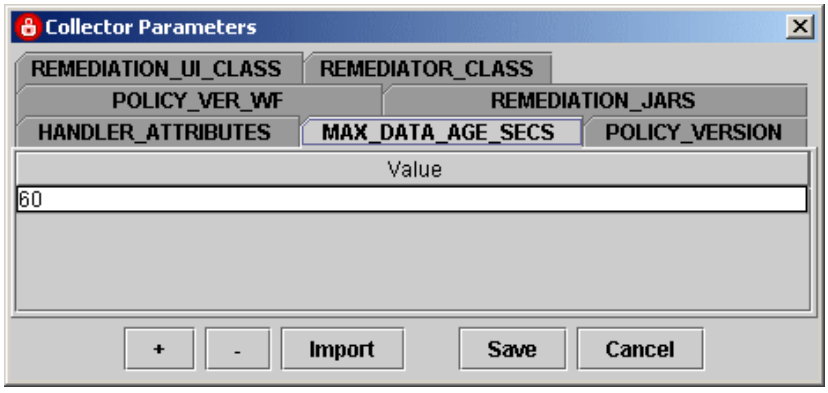


Figure 5-7 Setting the posture cache maximum data age

Downloaded from www.Manualslib.com manuals search engine

For ABBC we set the parameter to 60 seconds. Effectively this forces the posture status to refresh itself at every challenge. Figure 5-8 shows the conceptual control flow for this parameter.

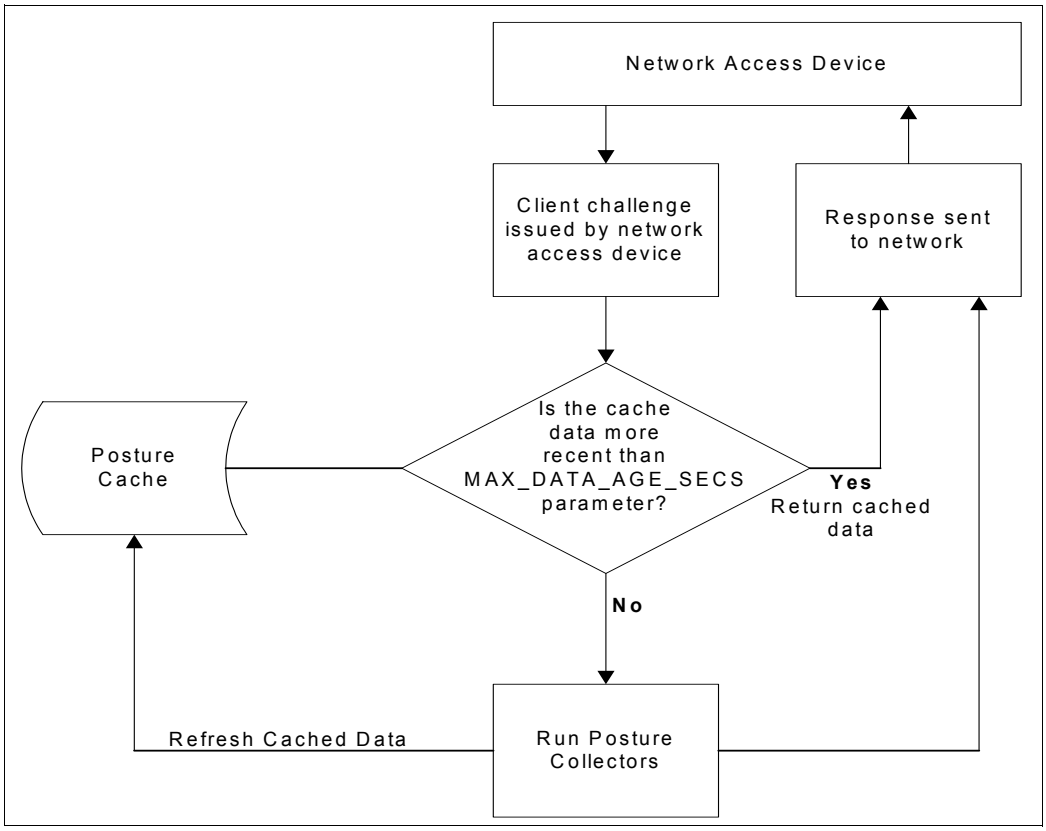


Figure 5-8 MAX_DATA_AGE_SECS conceptual flow

Downloaded from www.Manualslib.com manuals search engine

- The HANDLER_ATTRIBUTES parameter (Figure 5-9) establishes the URL where the remediation handler will send the remediation request, as well as more attributes for the remediation handler. This field has to have a form of <attribute_name>=<value> string, as presented below:

  ```
  remediation.url=http://tcmweb/SoftwarePackageServerWeb/SPServlet
  ```

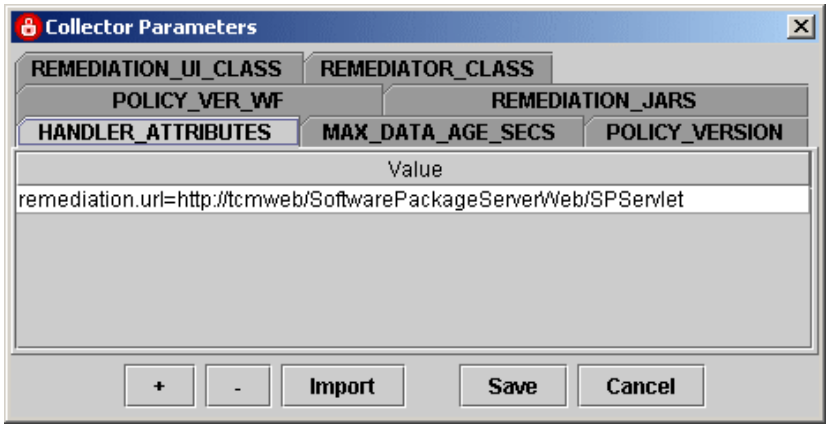


Figure 5-9 Setting the remediation handler URL attribute

- The REMEDIATOR_CLASS parameter (Figure 5-10) tells the policy collector which Java class to call to handle the remediation process. This field is a simple string and should have the value of:

  ```
  com.ibm.scm.nac.tcmremed.client.TCMRemediator
  ```

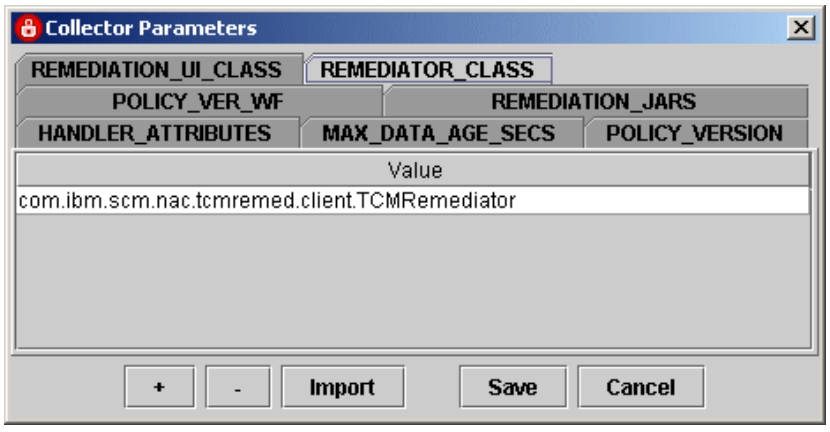


Figure 5-10 Setting the remediation handler class name

Downloaded from www.Manualslib.com manuals search engine

- The REMEDIATOR_JAR parameter (Figure 5-10 on page 108) tells the class loader where the JAR file is located for the remediation Java class specified in the REMEDIATION_CLASS attribute. This field is a simple string and should have the value of:

  `collectors/com.ibm.scm.nac.tcmremed.client.TCMRemed.jar`

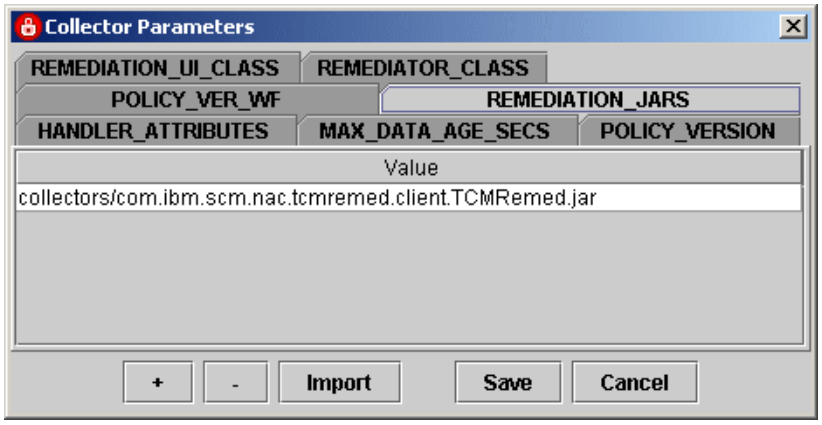


Figure 5-11 Setting the remediation handler JAR classpath

The value of the POLICY_VERSION parameter must then be handed over to the networking team.

Enforcing compliance criteria

Now we must configure the Cisco Secure Access Control Server policy.

In Chapter 3, “Component structure” on page 39, we discussed the various components, subcomponents, and transport mechanisms involved in this solution. In “Posture validation and policy enforcement” on page 59 we discussed the mechanics of *how* the posture validation process is conducted. Here, we

Downloaded from www.Manualslib.com manuals search engine

focus on how our posture policy, as established by the Tivoli Security Compliance Manager, interrelates with the Cisco Secure Access Control Server and how its associated polices form an interlocked security solution (Figure 5-12).

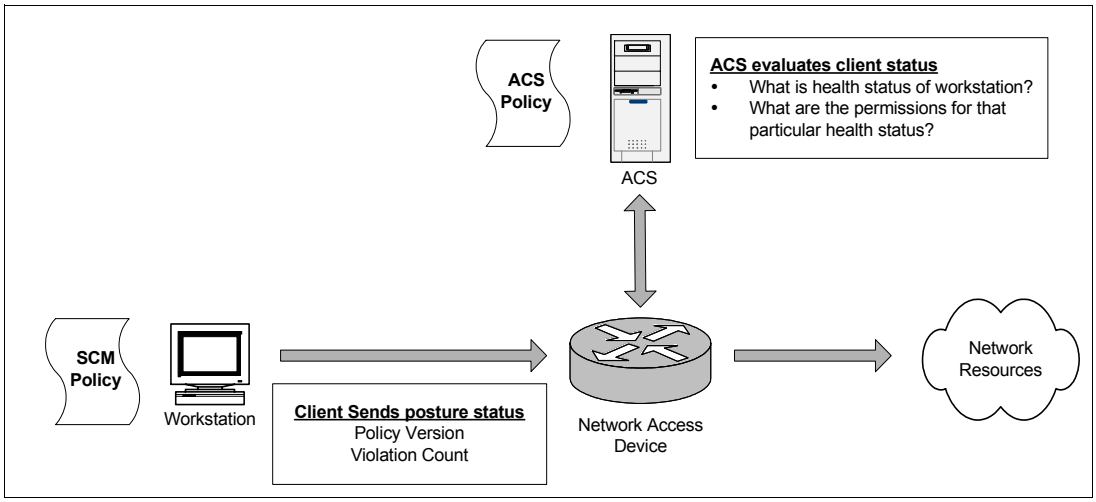


Figure 5-12 Simplified policy interrelations

Posture token

For all of the moving parts and pieces, at the time of this writing[1], only two pieces of posture status information are transmitted from the Security Compliance Manager posture client to the network:

- The *version* of the posture policy the client is running. This parameter is a string value and is established at the time of policy collection. We set this value in “Establishing the policy collector parameters” on page 104.
- The *violation count*, which is the total sum of all violations found by the posture collector policies assigned to the client.

[1] Enhancements *may* be seen in future releases, including finer-grained posture data transmission.

Downloaded from www.Manualslib.com manuals search engine

In the posture validation policies, we check that a client has the correct minimum supported version of CTA installed and is running the correct version of the Security Compliance Manager policy (Figure 5-13).

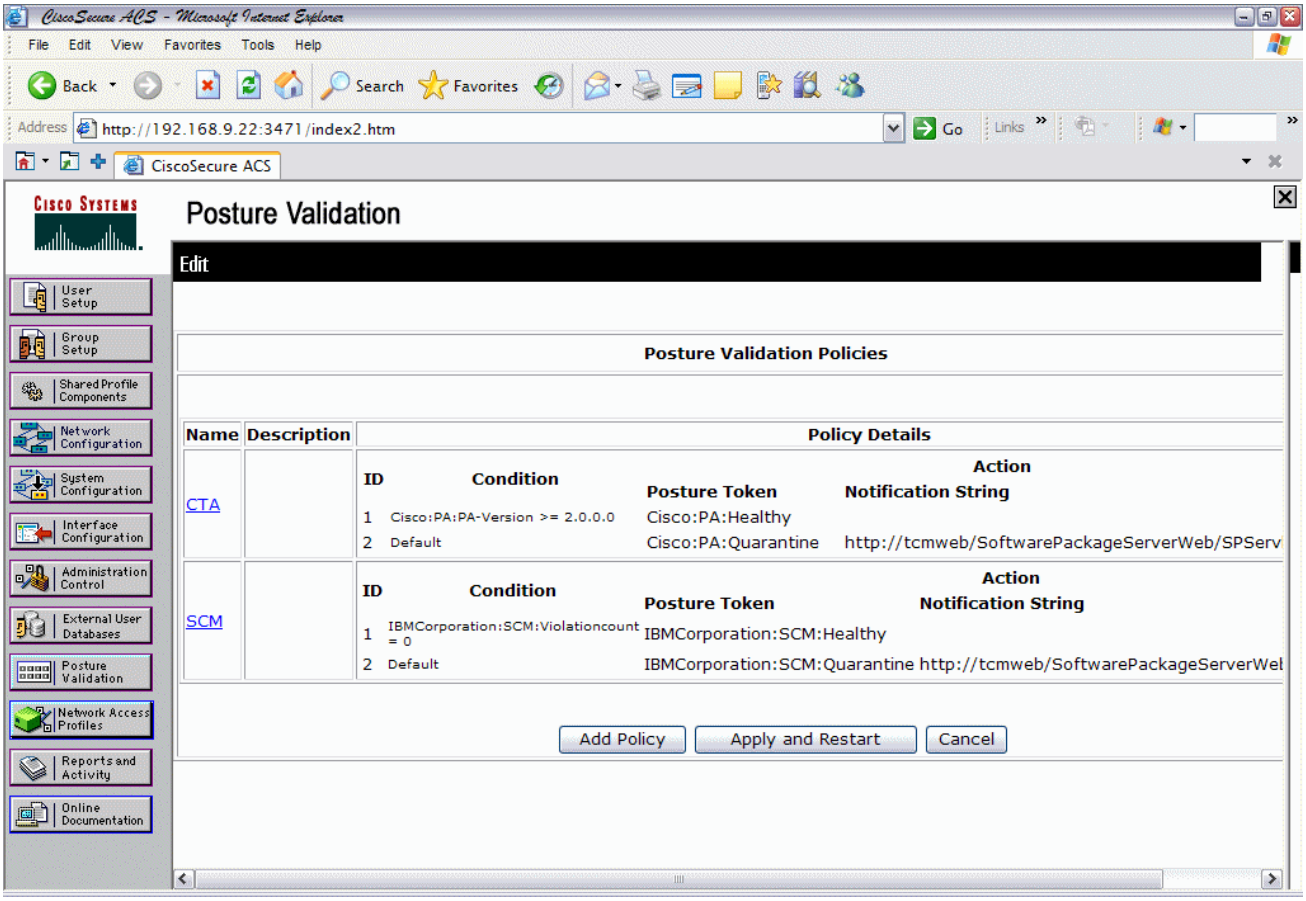


Figure 5-13 Posture validation policies

For detailed information about the creation and configuration of the Cisco Secure Access Control Server reference see 7.1.1, “Configuring the Cisco Secure ACS for NAC L2 802.1x” on page 214. This section discusses the way the policy is evaluated.

After setting the posture validation requirements, which essentially are the mandatory requirements to access the network, we must decide what to do with

Downloaded from www.Manualslib.com manuals search engine

those users that are in breach of these requirements, and how to remediate them back to a compliant state.

Terms that are used include:

- Network Access Profile

  A Network Access Profile is a means to classify access requests according to AAA clients' IP addresses, membership in a network device group, protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.

  A Network Access Profile is comprised of three components: Authentication, Posture Validation and Authorization.

- RADIUS Authorization Components

  Shared RADIUS Authorization Components (RACs) are configurable sets of RADIUS attributes that may be assigned to user or user group sessions dynamically based on a policy.

- Posture validation

  An internal posture validation policy returns a posture token after checking the rules set for the policy. Internal policies are reusable and can be used for posture validation for more than one Network Access Profile.

By supporting Layer 2 NAC we can enforce endpoint compliance on the LAN by using Cisco switches. There are two methods of NAC enablement: NAC L2 IP, which uses EAPoUDP; and NAC L2 802.1x, which uses an IEEE 802.1X supplicant embedded in the Cisco Trust Agent to provide machine and user authentication. This is the most secure form of L2 NAC, as now we are checking *who* is connecting to our networks as well as *what* is connecting to our networks.

In our scenario, we focus on the NAC L2 802.1x implementation of NAC. We have defined some user groups and users who have been assigned to those groups.

When a user connects to the network, she is prompted for the IEEE 802.1x credentials, in the form of a user name and password. Upon entering these credentials, the user is then mapped to the respective user group. The ACS then receives the posture credentials from the Cisco Trust Agent installed on the client. Based on the System Posture Token, the user is then mapped to a Shared RADIUS Authorization Component. Part of this Shared RADIUS Authorization Component is the VLAN that the user is assigned to.

An example of this is as follows. Jim is a member of the Engineering Group. When Jim logs on, he successfully authenticates to IEEE 802.1x. His posture assessment is *Healthy*, so Jim is mapped to the Healthy_Engineering_RAC (VLAN 12). Should Jim pass his IEEE 802.1x authentication, but receive a

Downloaded from www.Manualslib.com manuals search engine

Quarantine System Posture Token for a policy violation, he will be mapped to the Quarantine_Engineering_RAC (VLAN14). This allows for scalability and granularity.

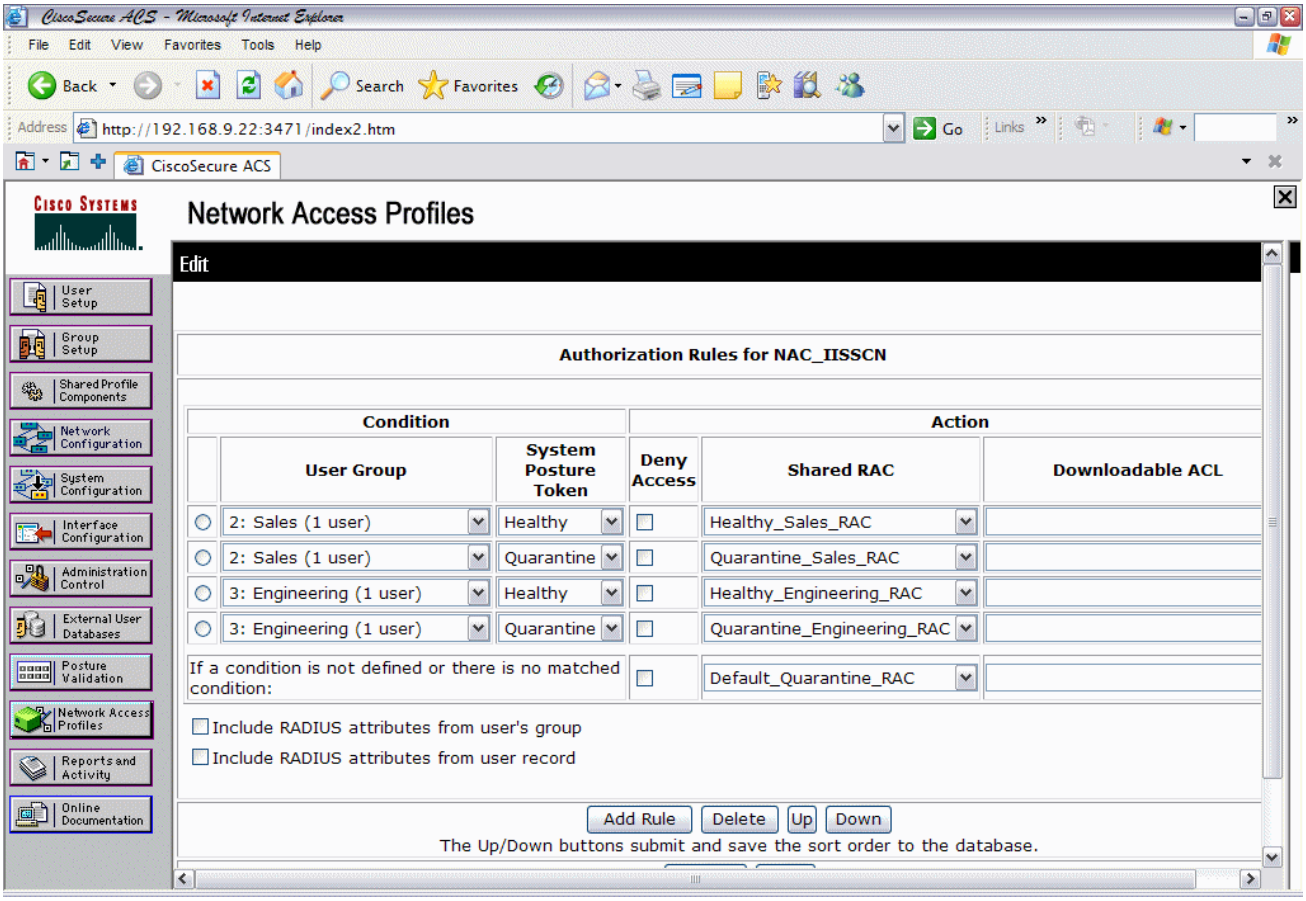


Figure 5-14 Shared RADIUS Authorization Components

In our scenario, we list the Cisco Trust Agent (Cisco:PA) and the Security Compliance Manager agent (IBM Corporation:SCM) as our posture validation policies. Thus in all, three pieces of information are used to make the access decision:

- IEEE 802.1x authentication (User Group Mapping)
- The Security Compliance Manager policy version
- The Security Compliance Manager posture policy violation count

Downloaded from www.Manualslib.com manuals search engine

The Cisco Secure ACS evaluates each of the authorization rules in order from top to bottom. The first match assigns the client the listed posture token. If no match is found, the default rule assigns the listed token.

Assigning the System Posture Token

Cisco Secure ACS supports the following System Posture Token types:

Healthy	The endpoint device complies with the currently required credentials so you do not have to restrict this device.
Checkup	The endpoint device is within the policy but does not have the latest security software. We recommend an update. Use to proactively remediate a host to the Healthy state.
Quarantine	The endpoint device is out of policy and must be restricted to a remediation network. The device is not actively placing a threat on other hosts, but is susceptible to attack or infection and should be updated as soon as possible.
Transition	The endpoint device is in the process of having its posture checked and is given interim access pending a result from a full posture validation. This is applicable during host boot where all services may not be running or while audit results are not yet available.
Infected	The endpoint device is an active threat to other hosts. Network access should be severely restricted and placed into remediation or totally denied all network access.
Unknown	The posture credentials of the endpoint device cannot be determined. Quarantine the host and audit, or remediate until a definitive posture can be determined.

In our scenario we only use Healthy and Quarantine. *Healthy* indicates that the system is in full compliance and is therefore granted full network access. *Quarantined* indicates that the system has a violation count of at least one and the system is denied access to the network until remediation has taken place. There should not be an *unknown* system in the ACS. This is because we are using IEEE 802.1x. Should the user fail IEEE 802.1x authentication, the user will not have any network access, or may be granted access to the guest VLAN configured on the switch, depending on your network policy, as in some situations it may be desirable to allow unknown systems access to the Internet (for example, visitors or contractors).

At the time of writing this book, downloadable Access Control Lists were not supported when using NAC L2 802.1x. Therefore, the Access Control Lists are defined on the NAD, in our case a Layer-3 capable Cisco 3750 switch. Switched Virtual Interfaces (SVIs) were defined, and the access lists were bound to these

Downloaded from www.Manualslib.com manuals search engine

SVIs. Each Shared RADIUS Authorization Component had a corresponding ACL defined on the NAD. The example below shows the configuration used for the Healthy Engineering VLAN and the Quarantine Sales VLAN.

```
access-list 120 remark **Healthy Engineering VLAN ACLs**
access-list 120 deny ip any 192.168.13.0 0.0.0.255
access-list 120 deny ip any 192.168.14.0 0.0.0.255
access-list 120 deny ip any 192.168.15.0 0.0.0.255
access-list 120 permit ip any any
!
access-list 130 remark **Quarantine Sales VLAN ACLs**
access-list 130 permit icmp any host 192.168.9.220
access-list 130 permit icmp any host 192.168.104.10
access-list 130 permit ip any host 192.168.9.220
access-list 130 permit ip any host 192.168.104.10
access-list 130 permit udp any eq bootpc any eq bootps
access-list 130 deny ip any 192.168.11.0 0.0.0.255
access-list 130 deny ip any 192.168.12.0 0.0.0.255
access-list 130 deny ip any 192.168.14.0 0.0.0.255
access-list 130 deny ip any 192.168.15.0 0.0.0.255
access-list 130 permit tcp any any eq www
access-list 130 permit tcp any any eq domain
access-list 130 deny ip any any log
!
```

Note that the Healthy Engineering VLAN ACL has three deny entries before the permit statement. This is to stop any member of this VLAN trying to initiate any connections to any of the Quarantine VLANs, as an added security measure.

Similarly, note that the Quarantine Sales VLAN ACL allows the Security Compliance Manager and Tivoli Configuration Manager to be pinged, as a check for network connectivity, and also allows IP access to just the Security Compliance Manager and Tivoli Configuration Manager. This is for receiving an updated policy and other automated remediation tasks.

Performing remediation

Now that the Security Compliance Manager and ACS policies have been configured, the next step is to prepare the appropriate remediation workflows.

The operations team based on the names of the workflows assigned during policy creation have to design and deploy the set of software package blocks also known as remediation packages or workflows on Tivoli Configuration Manager server. These steps require the remediation server to be installed and operational. Detailed procedures for setting up the remediation server are described in Chapter 8, “Remediation subsystem implementation” on page 355.

Downloaded from www.Manualslib.com manuals search engine

See 8.4, “Building the remediation workflows” on page 417, for information about the creation of the workflows for the IBM Integrated Security Solution for Cisco Networks.

Remediation handler HTML pages

The remediation process does not link back to a central *policy* as do the security compliance posture and the Access Control Server posture token and access control list. The compliance client provides a way to display HTML-based information to the user. This mechanism relies on locally based HTML content staged in specific client directories. When presented to the user, the user in turn can personally resolve the noncompliance issue with this information, or call the automated remediation if needed. However, it must be noted that managing the remediation help files is a *process* that includes these steps:

1. Understanding the policy posture compliance criteria.
2. Creating the informational HTML pages used by the compliance client to display detailed information to the user. For more information refer to Chapter 8, “Remediation subsystem implementation” on page 355.
3. Distributing the HTML pages to the client systems.

At the time of writing this book, there is no Security Compliance Manager in-band mechanism for distributing the HTML pages. Therefore the security administrator must rely on other mechanisms for both the initial distribution of the HTML pages and future updates. As a best practice, the HTML pages should be incorporated into the standard gold-disk images for new client workstations being deployed. In the absence of an automatic remediation subsystem, any HTML page updates must be distributed using an out-of-band tool or process. However, with the addition of the automatic remediation subsystem a distribution workflow can be put in place to update the HTML pages as necessary (this exercise is left for the reader.)

You can also bundle updated HTML pages into the policy collector JAR file. If you do this, they can be deployed automatically with a new or updated policy.

5.3.2 Physical components

Referencing Figure 5-3 on page 102, note that the solution is comprised of three major subsystems: the compliance subsystem, the Network Admission Control subsystem, and the remediation subsystem. In this section we delve further into the various physical components comprising each of the these subsystems.

Downloaded from www.Manualslib.com manuals search engine

Compliance subsystem

The compliance subsystem has two major components:

- The IBM Security Compliance Manager server
- The IBM Security Compliance Manager client

IBM Security Compliance Manager server

The required IBM Security Compliance Manager server software is Version 5.1.1 (at the time we are writing this book this version is also known as Version 5.1.0 Fix Pack 30).

The Security Compliance Manager server runs on a variety of supported platforms, which Table 5-1 lists.

Table 5-1 Supported server platforms for Security Compliance Manager server

Operating system	Level	OS patch/maintenance level
AIX®	5.2, 5.3	No fix pack required
Windows 2000	Server, Advance Server	Latest fix pack level
Windows 2003 Server	Standard Edition, Enterprise Edition	Latest fix pack level
Sun™ Solaris™	2.8, 2.9, 10	Latest fix pack level
SUSE Linux Enterprise Server for IA32 platform	8, 9	Latest fix pack level
Red Hat AS/ES 4.0 for IA32	4.0	Latest fix pack level

This list may change as new platforms and versions are being certified for support. For the latest list check the IBM Support Web site at:

http://www.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html

Lists of the hardware requirements for all of the different hardware architecture types are also available on the support Web page at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itscm.doc_5.1/toc.xml

Consult this site for the final authority on specifications.

Downloaded from www.Manualslib.com manuals search engine

The system used by ABBC for the Security Compliance Manager server is:

- Windows 2003 Server Enterprise Edition with SP1 installed
- Pentium® IV @ 3.0Ghz CPU
- 512 MB of system memory
- 3 GB of free disk space

IBM Tivoli Security Compliance Manager client

The required IBM Security Compliance Manager client software is Version 5.1.1 (also known as 5.1.0 Fix Pack 30). This version contains the DLLs required to enable the Cisco integration.

With this version the client and server components are using different Java runtime environment versions and the installation packages for Security Compliance Manager server and Security Compliance Manager client components were separated. Although Security Compliance Manager supports many platforms as clients, the Cisco Trust Agent supports only Windows and Linux systems at this time.

Note: There are specific sequence requirements for the installation of the Cisco Trust Agent, the Security Compliance Manager client code. Refer to 6.3, “Deploying the client software” on page 189, for full details.

The system used by ABBC for the Security Compliance Manager client is:

- Windows XP professional with SP2 installed
- Pentium IV @ 3.0Ghz CPU
- 512 MB of system memory
- 3 GB of free disk space

Network Admission Control subsystem

The Network Admission Control (NAC) subsystem has three components:

- The Access Control Server (ACS)
- A NAC-enabled network device (for example, a switch)
- The Cisco Trust Agent with or without IEEE802.1x supplicant

Find additional information and individual component descriptions in 3.1.1, “Network Admission Control” on page 41. In this section we provide more details for each of the components as they relate to this solution implementation.

Access Control Server

The IBM Integrated Security Solution for Cisco Networks requires Version 4.0 of the Cisco Secure ACS. Detailed specifications follow.

Downloaded from www.Manualslib.com manuals search engine

Operating system requirements for ACS V4.0 are:

- Windows 2000 Server
- Windows 2000 Advanced Server with the following conditions:
  - Service Pack 4 installed
  - Without any feature specific to Windows 2000 Advanced Server enabled or without Microsoft clustering service enabled
- Windows Server® 2003, Enterprise Edition with Service Pack 1
- Windows Server 2003, Standard Edition with Service Pack 1

These requirements are from *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows 4.0,* which is found at (requires CCO login):

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_device_support_table09186a00805790b8.html

Per the *Installation Guide for Cisco Secure ACS for Windows Server Version 4.0*, the Access Control Server must comply to these minimum hardware specifications:

- Pentium IV CPU at 1.8 Ghz or faster
- 1 GB of system memory
- 1GB of virtual memory
- At least 1GB of free disk space
- Minimum supported graphics resolution of 256 colors at 800x600 resolution
- 100BaseT or faster network connection

This installation guide is found at (requires CCO login):

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_installation_guide_book09186a0080533d5e.html

Note: The specifications listed here are the official Cisco minimum requirements. However, for obvious reasons we would not recommend using such an underpowered system in a production environment.

ABBC used the following system for the Cisco Secure ACS:

- Windows 2000 Server with SP4 installed
- Pentium IV @ 3.0Ghz CPU
- 512 MB of system memory
- 3 GB of free disk space

Downloaded from www.Manualslib.com manuals search engine

NAC-enabled network device

The following Layer 2 and Layer 3 network devices are supported for a Network Admission Control implementation.

Layer 2 devices

Table 5-2 shows the supported Layer 2 devices.

Table 5-2 Layer 2 devices

NAC features	NAC Layer 2 IEEE 802.1x authentication and validation	NAC Layer 2 IP validation
7600	X	X
6500	X	X
4500	X	X
3750 Metro	-	-
3750	X	X
3560	X	X
3550 (12.2S)	X	X
3550 (12.1S)	X	-
2970	X	-
2960	X	-
2955	X	-
2950 -LRE	-	-
2950	X	-
2940	X	-
Cisco Aironet	X	-

Layer 3 devices

The following list shows the supported Layer 3 devices if they use Cisco IOS Software Release 12.3(8)T or later with Advanced Security feature set or greater.

- Cisco 83x Series Router
- Cisco 850 Series Router
- Cisco 870 Series Router
- Cisco 1700 Series Router
- Cisco 1800 Series Router

Downloaded from www.Manualslib.com manuals search engine

- Cisco 2600XM Series Router
- Cisco 2691 Multiservice Platform
- Cisco 2800 Series Router
- Cisco 3640 Multiservice Platform
- Cisco 3660-ENT Series Router
- Cisco 3725 and 3745 Multiservice Access Routers
- Cisco 3800 Series Router
- Cisco 7200 Series Router

For the most up-to-date information refer to:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c649/cdccont_0900aecd8040bc84.pdf

Cisco Trust Agent

The Cisco Trust Agent 2.0 with the IEEE 802.1x supplicant has the following software requirements:

- Microsoft Windows 2000 Professional (Service Pack 4 or later)
- Microsoft Windows 2000 Server (Service Pack 4 or later)
- Microsoft Windows 2000 Advanced Server (Service Pack 4 or later)
- Microsoft Windows XP Professional (Service Pack 1 or 2)
- Microsoft Windows 2003 Server, Standard Edition (Service Packs 0 and 1)
- Microsoft Windows 2003 Server, Enterprise Edition (Service Packs 0 and 1)
- Microsoft Windows 2003 Server, Web Edition (Service Packs 0 and 1)

The Cisco Trust Agent 2.0 has the following minimum hardware requirements:

- Single or multiple Pentium processors, 200 MHz or faster
- 128 MB RAM minimum for Windows 2000, 256 MB RAM minimum for Windows XP
- 5 MB of available hard disk space, 20 MB recommended
- Network connection

For the most up-to-date information refer to (requires CCO login):

http://www.cisco.com/en/US/partner/products/ps5923/products_maintenance_guide_chapter09186a008059a95f.html

Note: For the scenarios described in this book we used CTA 2.0.0.30 with IEEE 802.1x supplicant.

Downloaded from www.Manualslib.com manuals search engine

Remediation subsystem

The remediation subsystem has three components:

- IBM Tivoli Configuration Manager server
- Software Package Web Server
- Remediation handler

IBM Tivoli Configuration Manager server

The Tivoli Configuration Manager supports a wide range of architecture types as well as a range of installation topologies (one-node, two-node, and three-node). The resulting multitude of combinations is well beyond the scope of this book.

While we wrote this book, the current version of the remediation server was 4.2.3. For the list of supported operating systems types consult the IBM Support Web site at:

http://www.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html

We assumed that ABBC has the base IBM Tivoli Configuration Manager Version 4.2.3 server installed and configured, as it is used by the Operations department for Software Distribution and Inventory.

In 8.2.2, “Tivoli Configuration Manager” on page 359, the installation of the additionally required *Web Gateway* component is performed. The system used by ABBC for the remediation server is configured as follows:

- Windows 2003 Server Enterprise Edition with SP1 installed
- Pentium IV @ 3.0Ghz CPU
- 1024 MB of system memory
- 4 GB of free disk space
- The following middleware components are installed as prerequisites:
  - WebSphere Application Server 5.1.1.11
  - IBM HTTP Server 1.3.28
  - DB2 Universal Database™ Enterprise Edition 8.2

Note: We have tested these components also on the RedHat Linux Enterprise Server 4.0 Update 4 running on the same type of server, but for the purpose of the book all of the images and paths were documented from the Windows installation.

Software Package Web Server

This J2EE™ application is the interface element between remediation handler and Tivoli Configuration Manager Web Gateway. It is delivered with IISSCN extension pack2 for Tivoli Configuration Manager in the form of an installable

Downloaded from www.Manualslib.com manuals search engine

EAR file. This application must be installed on the same WebSphere Application Server as the Web Gateway component.

Remediation handler

In the current release of the solution, the remediation handler is delivered in the form of the Security Compliance Manger collector JAR file and is automatically downloaded to the client workstation together with the compliance policy. See 8.1, “Automated remediation enablement” on page 357, for more detailed configuration information.

5.4 Conclusion

In this chapter we described how the business objectives are combined with the pain points to drive a set of functional requirements. We then explored the functional requirements to effectively map them to a technology solution.

Compliance-based Network Admission Control is still an emerging technology that brings with it a huge paradigm shift in network security management. There are three main parts outlined in this chapter. In part one, the security compliance infrastructure is established, allowing the workstations to be validated against a desktop security policy checking on password quality, unauthorized Windows services, antivirus statistics, personal firewall status, and installed hotfixes. In Part 2, “Customer environment” on page 75, the Network Admission Control technology is utilized for user authorization and limiting the network access for noncompliant clients. In Part 3, “Appendixes” on page 439, we provide the infrastructure for automatic remediation of noncompliant systems before they are admitted to the secure network.

In the chapters that follow we provide detailed installation and configuration walkthroughs. These walkthroughs drill down further into the specifics, such as installing and configuring the server components, the client components, and the automatic remediation subsystem.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

6

Compliance subsystem implementation

This chapter describes the IBM Tivoli Security Compliance Manager part of the Network Admission Control (NAC) solution, where the main concern is the establishment of security policy.

We describe the process of setting up the compliance components, which includes:

- Installation and configuration of Tivoli Security Compliance Manager server
- Installation of the policy collector and the Tivoli Configuration Manager-based remediation handler collectors onto the Tivoli Security Compliance Manager server
- Configuration of the security compliance policy for the desktops. There are two major parts:
  - Providing the policy with the suitable remediation workflow names and parameters
  - Assigning the policy to Security Compliance Manager clients
- Deployment of the client software, which includes two parts:
  - Installation of the Cisco Trust Agent Software
  - Installation of the Tivoli Security Compliance Manager client

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

6.1 Tivoli Security Compliance Manager setup

Tivoli Security Compliance Manager server is an important component of the solution providing the policy management service to the client workstations. In the section below we describe the process of installing the Tivoli Security Compliance Manager server.

To perform the installation the following media are needed:

- DB2 Universal Database 8.2
- Tivoli Security Compliance Manager Server 5.1.1

Note: The Tivoli Security Compliance Manager Server 5.1.1 is the new base installation image, which means that you do not need any previous version to install Tivoli Security Compliance Manager. At the time we wrote this book it was also known as Version 5.1.0 Fix Pack 30. One of the important differences is the fact that now server and client installation files were divided into two separate CD images.

6.1.1 Installation of DB2 database server

DB2 Universal Database software should be included with the Tivoli Security Compliance Manager installation bundle, and it is a prerequisite that it be installed first. Follow the below steps to install the DB2 database.

Important: DB2 installation must be performed from the local hard drive or from the CD. If you try to install from a Windows shared network drive the installation will fail. Copy the installation files to the local drive instead.

1. To start the installation move to the directory where you have copied the binaries and run the setup file db2setup.exe.

Downloaded from www.Manualslib.com manuals search engine

2. After a little while you are presented with the Welcome window, as shown in Figure 6-1. Click the **Install Product** selection on the left.

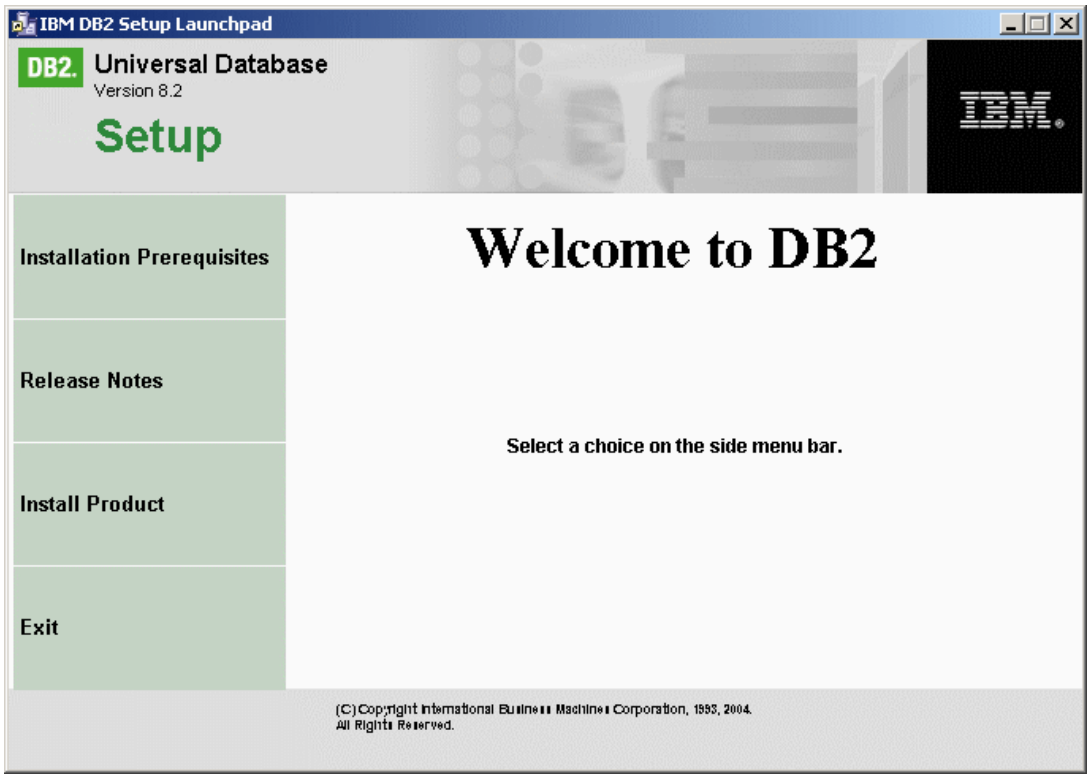


Figure 6-1 DB2 installation welcome window

Downloaded from www.Manualslib.com manuals search engine

3. The DB2 version selection is presented similar to the one shown in Figure 6-2. Depending on the media installation you use there may be more than one option presented. Select **DB2 UDB Enterprise Server Edition** and click **Next**.

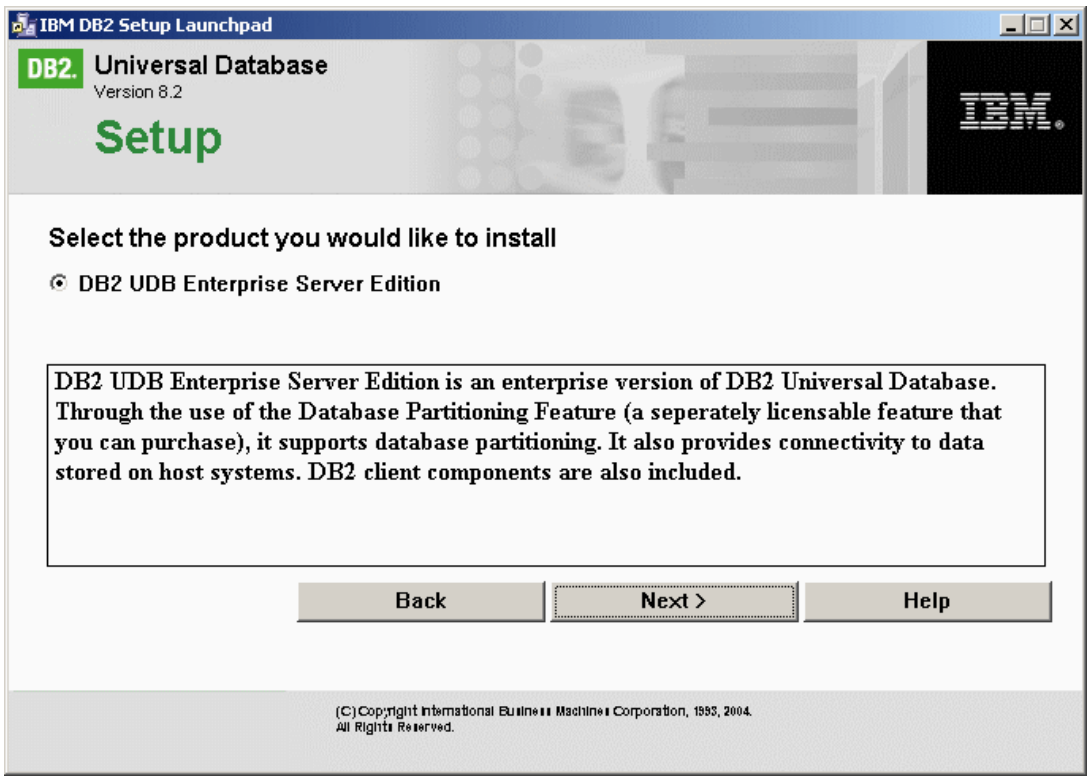

IBM DB2 Setup Launchpad
DB2
Universal Database
Version 8.2
Setup
IBM
Select the product you would like to install
DB2 UDB Enterprise Server Edition
DB2 UDB Enterprise Server Edition is an enterprise version of DB2 Universal Database. Through the use of the Database Partitioning Feature (a seperately licensable feature that you can purchase), it supports database partitioning. It also provides connectivity to data stored on host systems. DB2 client components are also included.
Back
Next >
Help
(C) Copyright International Business Machines Corporation, 1993, 2004.
All Rights Reserved.

Figure 6-2 DB2 version selection window

Downloaded from www.Manualslib.com manuals search engine

4. Next the welcome window is displayed, as presented in Figure 6-3. Click **Next**.

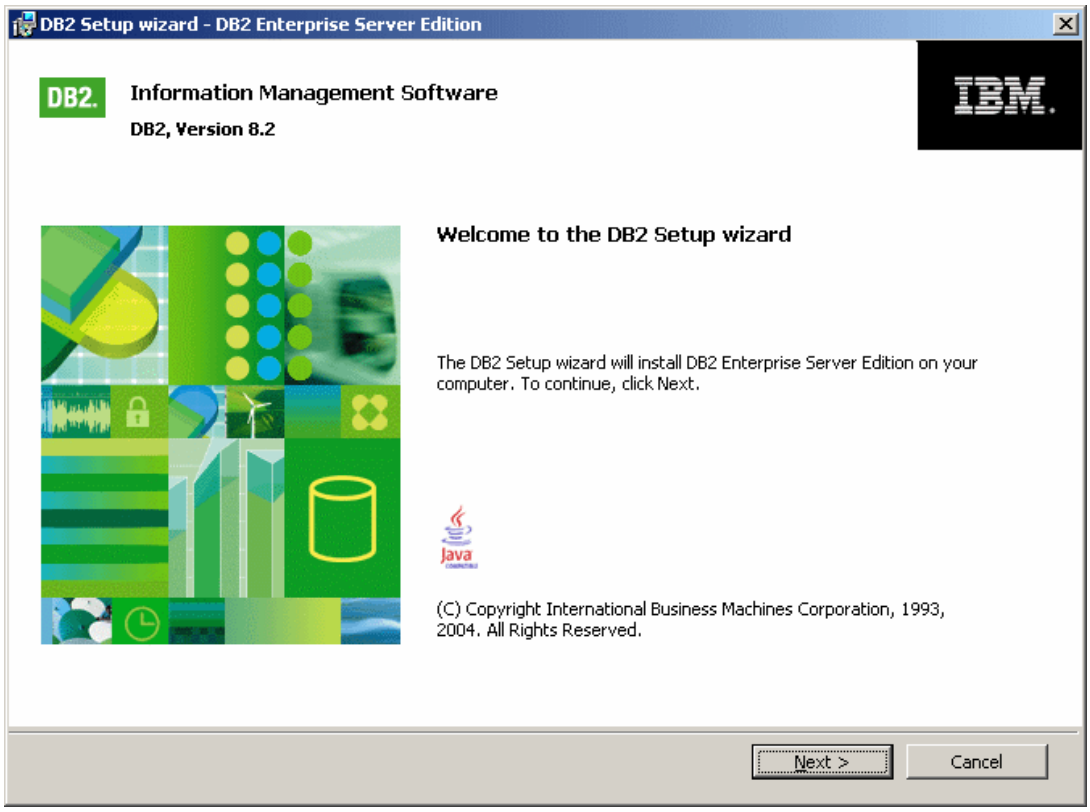

DB2 Setup wizard - DB2 Enterprise Server Edition
DB2.
Information Management Software
DB2, Version 8.2
IBM.
Welcome to the DB2 Setup wizard
The DB2 Setup wizard will install DB2 Enterprise Server Edition on your computer. To continue, click Next.
Java
(C) Copyright International Business Machines Corporation, 1993, 2004. All Rights Reserved.
Next >
Cancel

Figure 6-3 Setup wizard welcome window

Downloaded from www.Manualslib.com manuals search engine

5. On the next dialog you are presented with the standard license agreement (Figure 6-4). Accept the license and click **Next**.

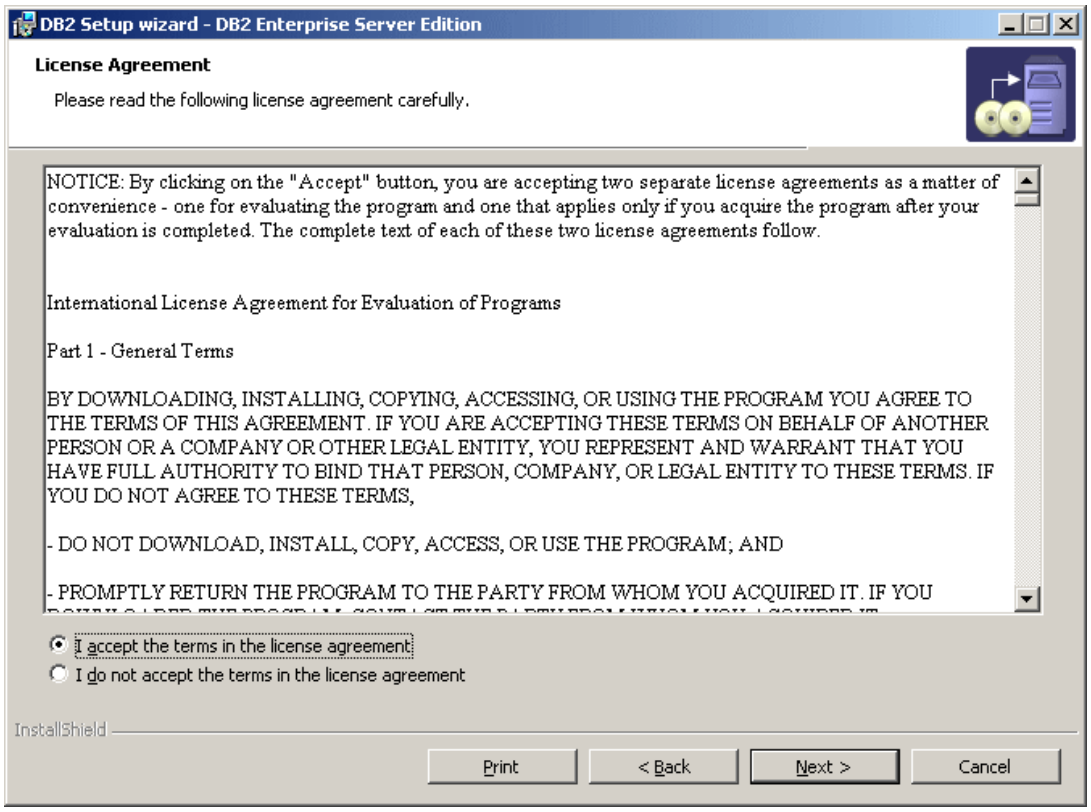

DB2 Setup wizard - DB2 Enterprise Server Edition
License Agreement
Please read the following license agreement carefully.
NOTICE: By clicking on the "Accept" button, you are accepting two separate license agreements as a matter of convenience - one for evaluating the program and one that applies only if you acquire the program after your evaluation is completed. The complete text of each of these two license agreements follow.
International License Agreement for Evaluation of Programs
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM TO THE PARTY FROM WHOM YOU ACQUIRED IT. IF YOU
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
Print
< Back
Next >
Cancel

Figure 6-4 License agreement window

Downloaded from www.Manualslib.com manuals search engine

6. In the Installation type selection window (Figure 6-5) leave all of the default values (which is *Typical* installation) and click **Next**.

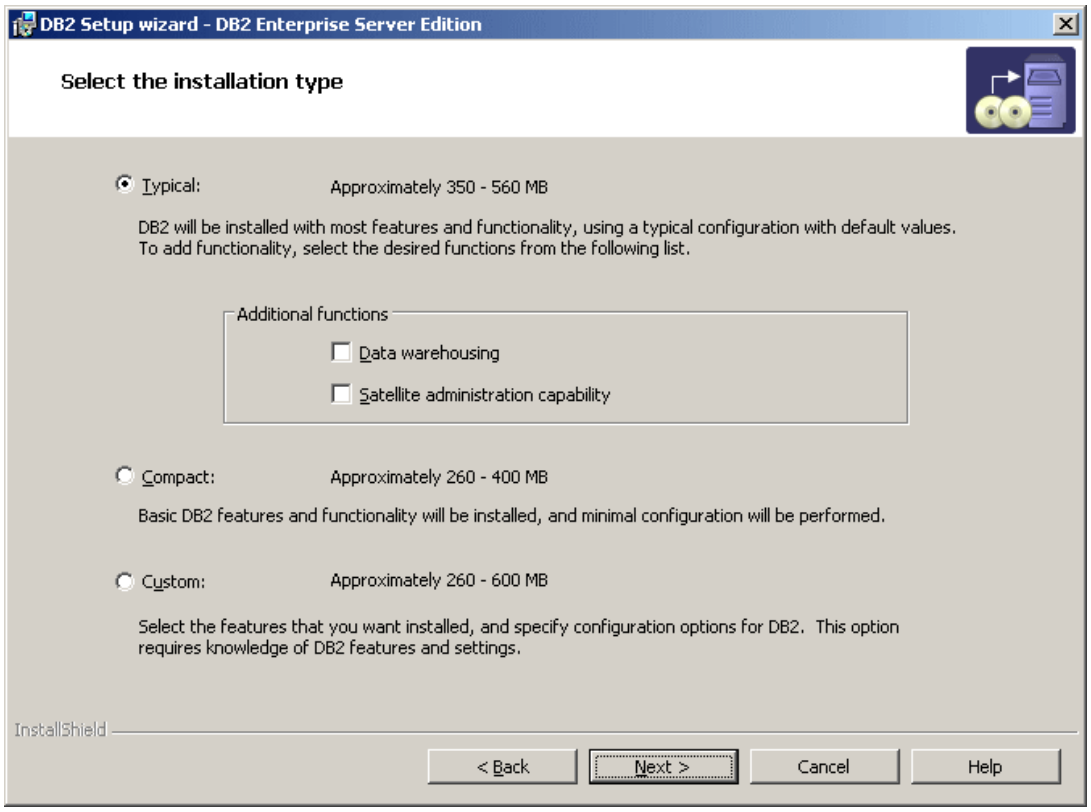

DB2 Setup wizard - DB2 Enterprise Server Edition
Select the installation type
Typical:
Approximately 350 - 560 MB
DB2 will be installed with most features and functionality, using a typical configuration with default values.
To add functionality, select the desired functions from the following list.
Additional functions
Data warehousing
Satellite administration capability
Compact:
Approximately 260 - 400 MB
Basic DB2 features and functionality will be installed, and minimal configuration will be performed.
Custom:
Approximately 260 - 600 MB
Select the features that you want installed, and specify configuration options for DB2. This option requires knowledge of DB2 features and settings.
InstallShield
< Back
Next >
Cancel
Help

Figure 6-5 Installation type selection window

Downloaded from www.Manualslib.com manuals search engine

7. On the next dialog, shown in Figure 6-6, you are presented with the installation action selection, where there are two options:

   Install the product Which is selected by default

   Save your settings Which will save your selections to a response file, which can then be used for silent installations

   If you plan to perform multiple installations you may mark the second check box. Otherwise, click **Next**.

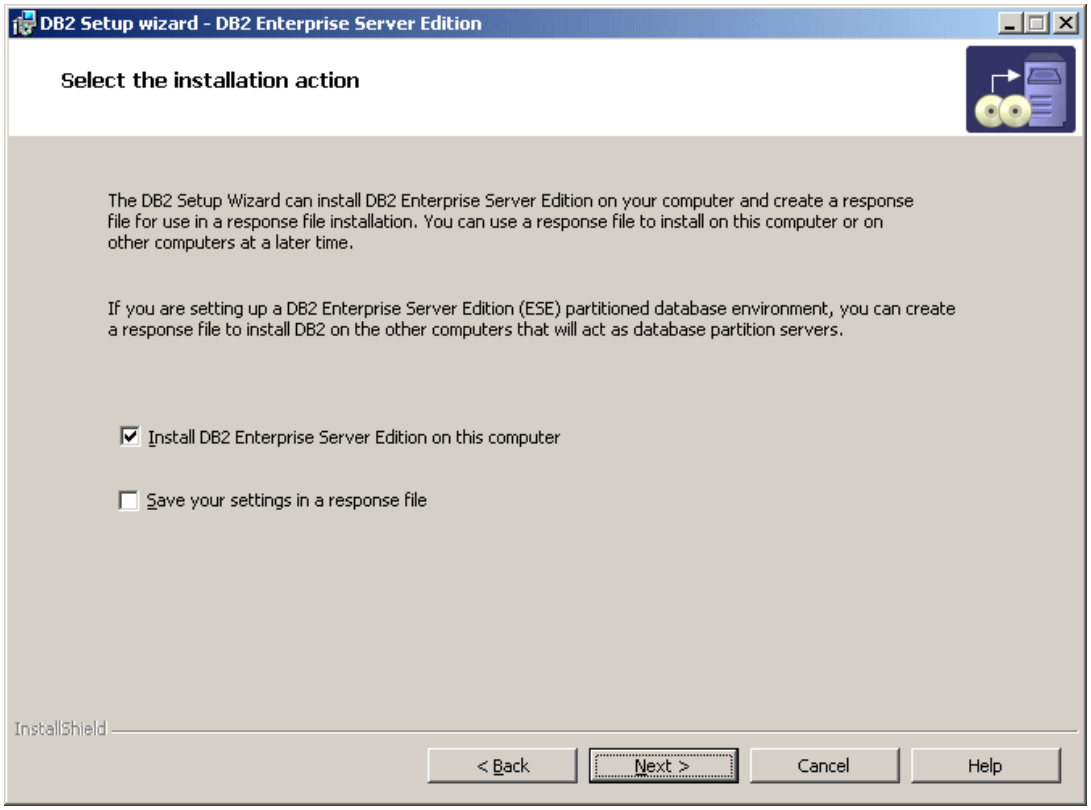

DB2 Setup wizard - DB2 Enterprise Server Edition
Select the installation action
The DB2 Setup Wizard can install DB2 Enterprise Server Edition on your computer and create a response file for use in a response file installation. You can use a response file to install on this computer or on other computers at a later time.
If you are setting up a DB2 Enterprise Server Edition (ESE) partitioned database environment, you can create a response file to install DB2 on the other computers that will act as database partition servers.
Install DB2 Enterprise Server Edition on this computer
Save your settings in a response file
InstallShield
< Back
Next >
Cancel
Help

Figure 6-6 Installation action selection window

Downloaded from www.Manualslib.com manuals search engine

8. In the next window, shown in Figure 6-7, you must select the installation destination folder. Make sure that there is enough space on the selected drive and click **Next**.

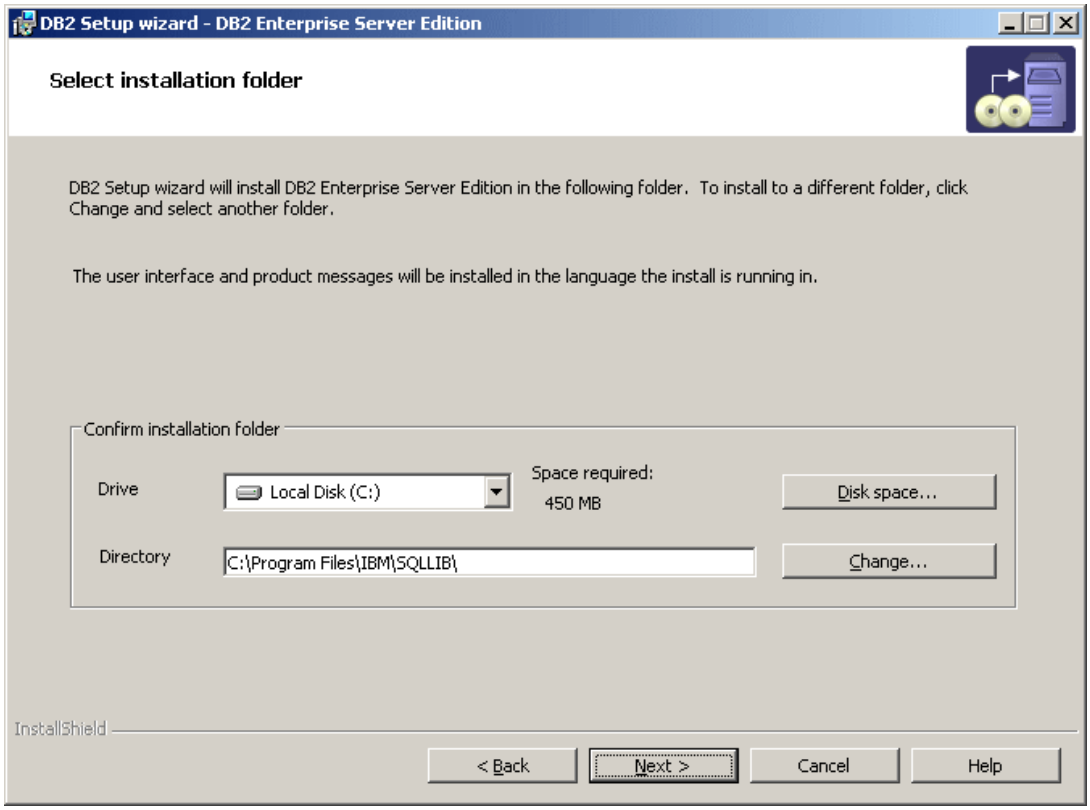

DB2 Setup wizard - DB2 Enterprise Server Edition
Select installation folder
DB2 Setup wizard will install DB2 Enterprise Server Edition in the following folder. To install to a different folder, click Change and select another folder.
The user interface and product messages will be installed in the language the install is running in.
Confirm installation folder
Drive
Local Disk (C:)
Space required:
450 MB
Disk space...
Directory
C:\Program Files\IBM\SQLLIB\
Change...
InstallShield
< Back
Next >
Cancel
Help

Figure 6-7 Installation folder selection window

Downloaded from www.Manualslib.com manuals search engine

9. In the next dialog, shown in Figure 6-8, you must provide user information. We strongly recommend leaving the default user name db2admin. In the next two fields provide the password for this user. Make sure that you have written this down, as you will need this password several times during the installation of the other components. Then click **Next**.

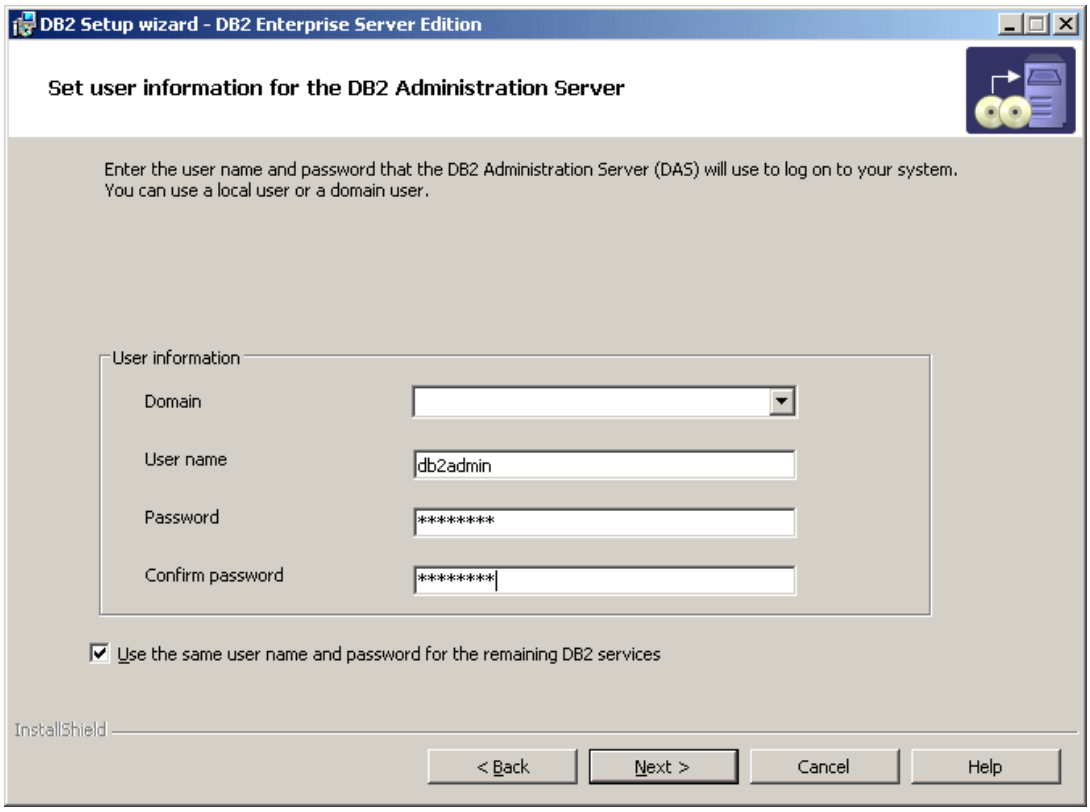

DB2 Setup wizard - DB2 Enterprise Server Edition
Set user information for the DB2 Administration Server
Enter the user name and password that the DB2 Administration Server (DAS) will use to log on to your system.
You can use a local user or a domain user.
User information
Domain
User name
db2admin
Password
Confirm password
Use the same user name and password for the remaining DB2 services
InstallShield
< Back
Next >
Cancel
Help

Figure 6-8 User information dialog

Downloaded from www.Manualslib.com manuals search engine

10. In the next dialog, depicted in Figure 6-9, you are presented with the administration contact configuration options, where you may specify names of the users who should be notified by the database if something goes wrong. If you leave the defaults and click **Next** you will be presented with the additional warning that `Notification SMTP server information has not been specified`, which you can ignore by clicking **OK**.

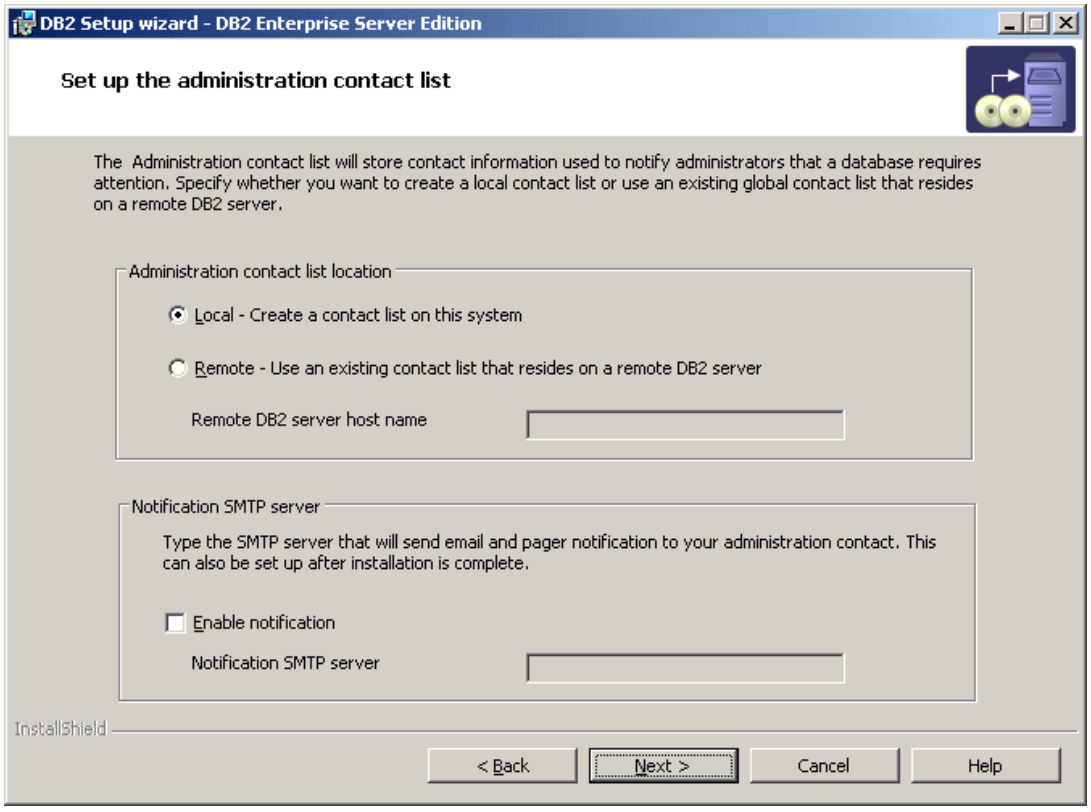

DB2 Setup wizard - DB2 Enterprise Server Edition
Set up the administration contact list
The Administration contact list will store contact information used to notify administrators that a database requires attention. Specify whether you want to create a local contact list or use an existing global contact list that resides on a remote DB2 server.
Administration contact list location
Local - Create a contact list on this system
Remote - Use an existing contact list that resides on a remote DB2 server
Remote DB2 server host name
Notification SMTP server
Type the SMTP server that will send email and pager notification to your administration contact. This can also be set up after installation is complete.
Enable notification
Notification SMTP server
InstallShield
< Back
Next >
Cancel
Help

Figure 6-9 Administration contact list dialog

Downloaded from www.Manualslib.com manuals search engine

11. In the next window, shown in Figure 6-10, you can modify the DB2 instance configuration options. You can explore the protocols settings and change the startup options. The default instance name on Windows is DB2, the communication protocol used is TCP/IP, and the database instance is instructed to start automatically when you boot the system. We recommend that you leave the defaults and click **Next**.

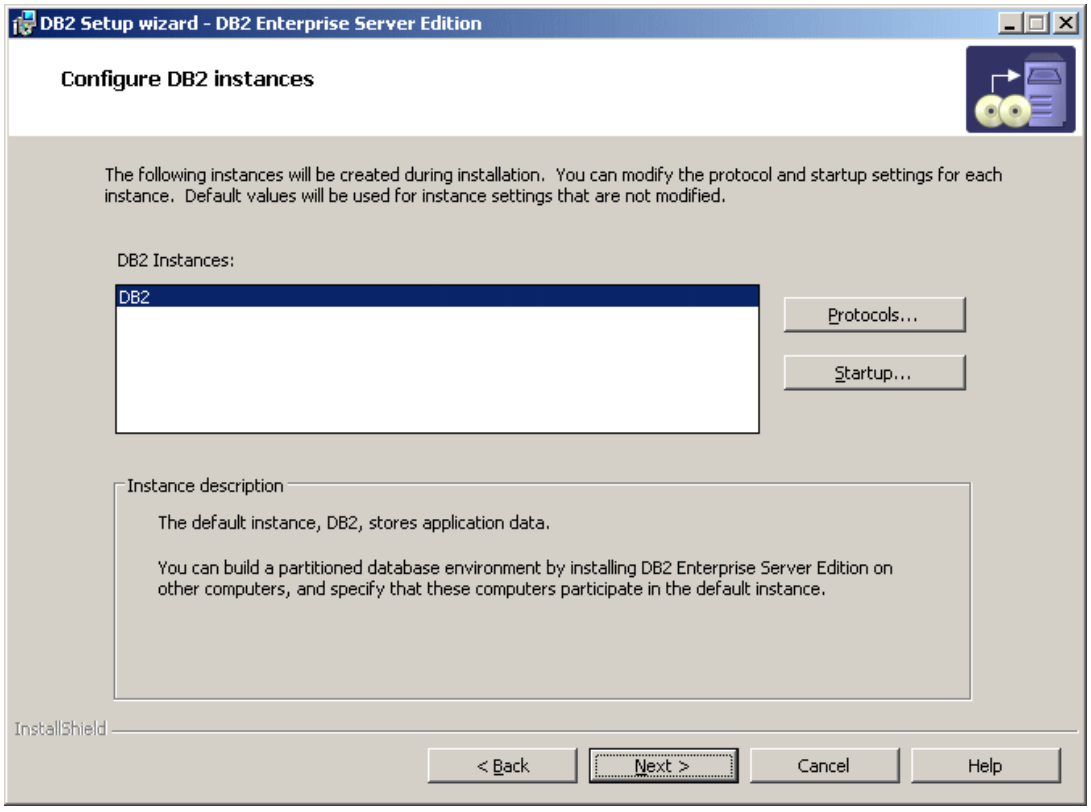

DB2 Setup wizard - DB2 Enterprise Server Edition
Configure DB2 instances
The following instances will be created during installation. You can modify the protocol and startup settings for each instance. Default values will be used for instance settings that are not modified.
DB2 Instances:
DB2
Protocols...
Startup...
Instance description
The default instance, DB2, stores application data.
You can build a partitioned database environment by installing DB2 Enterprise Server Edition on other computers, and specify that these computers participate in the default instance.
InstallShield
< Back
Next >
Cancel
Help

Figure 6-10 DB2 Instance configuration window

Downloaded from www.Manualslib.com manuals search engine

12. As we do not need to use any DB2 tools on the next dialog, shown in Figure 6-11, click **Next**.

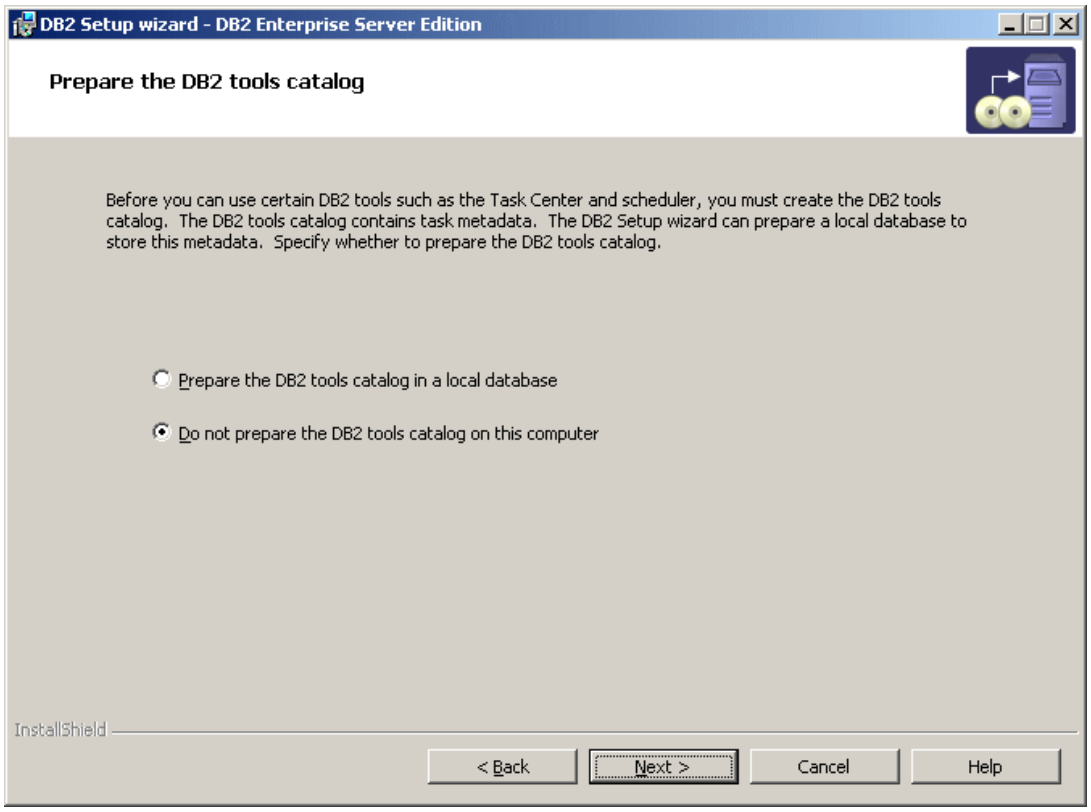

DB2 Setup wizard - DB2 Enterprise Server Edition
Prepare the DB2 tools catalog
Before you can use certain DB2 tools such as the Task Center and scheduler, you must create the DB2 tools catalog. The DB2 tools catalog contains task metadata. The DB2 Setup wizard can prepare a local database to store this metadata. Specify whether to prepare the DB2 tools catalog.
Prepare the DB2 tools catalog in a local database
Do not prepare the DB2 tools catalog on this computer
InstallShield
< Back
Next >
Cancel
Help

Figure 6-11 DB2 Tools selection dialog

Downloaded from www.Manualslib.com manuals search engine

13. In the next window, presented in Figure 6-12, you can provide the contact information for a user to receive the database health notifications. Select the option to **Defer this task until after installation is complete** and click **Next**.

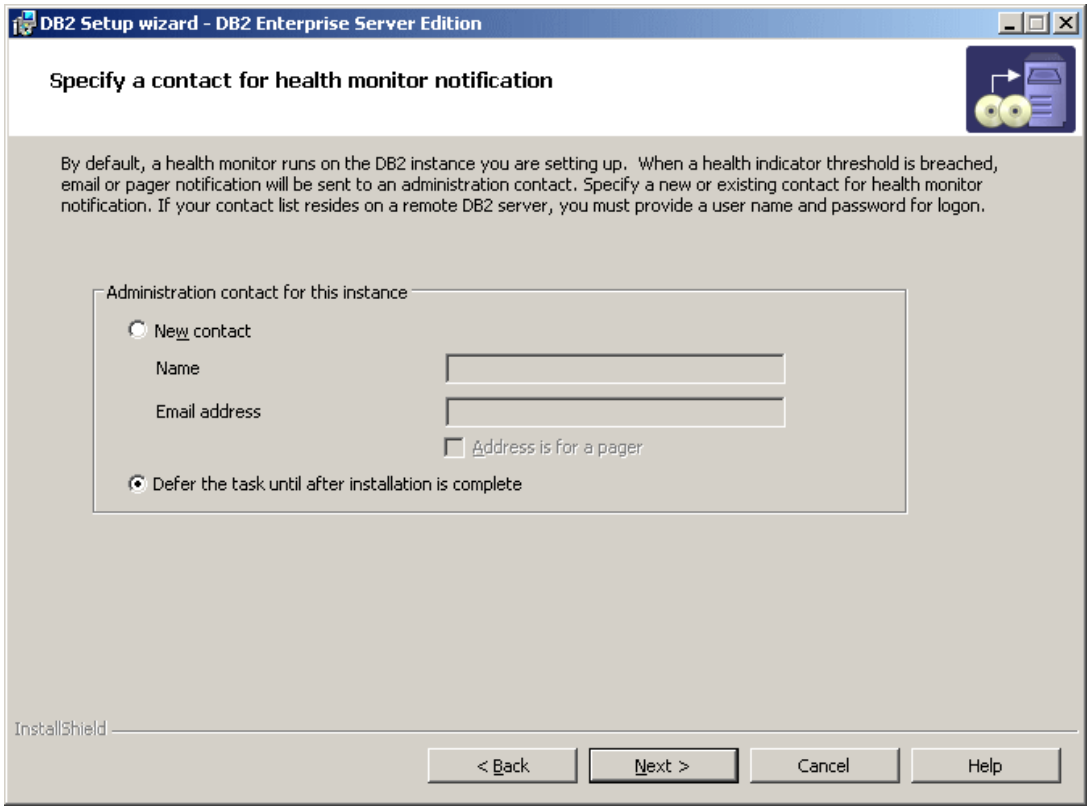

DB2 Setup wizard - DB2 Enterprise Server Edition
Specify a contact for health monitor notification
By default, a health monitor runs on the DB2 instance you are setting up. When a health indicator threshold is breached, email or pager notification will be sent to an administration contact. Specify a new or existing contact for health monitor notification. If your contact list resides on a remote DB2 server, you must provide a user name and password for logon.
Administration contact for this instance
New contact
Name
Email address
Address is for a pager
Defer the task until after installation is complete
InstallShield
< Back
Next >
Cancel
Help

Figure 6-12 Administrator contact selection window

Downloaded from www.Manualslib.com manuals search engine

14. In the next window, shown in Figure 6-13, you are given a last chance to review your selected options. If everything is as you want, click **Install**.

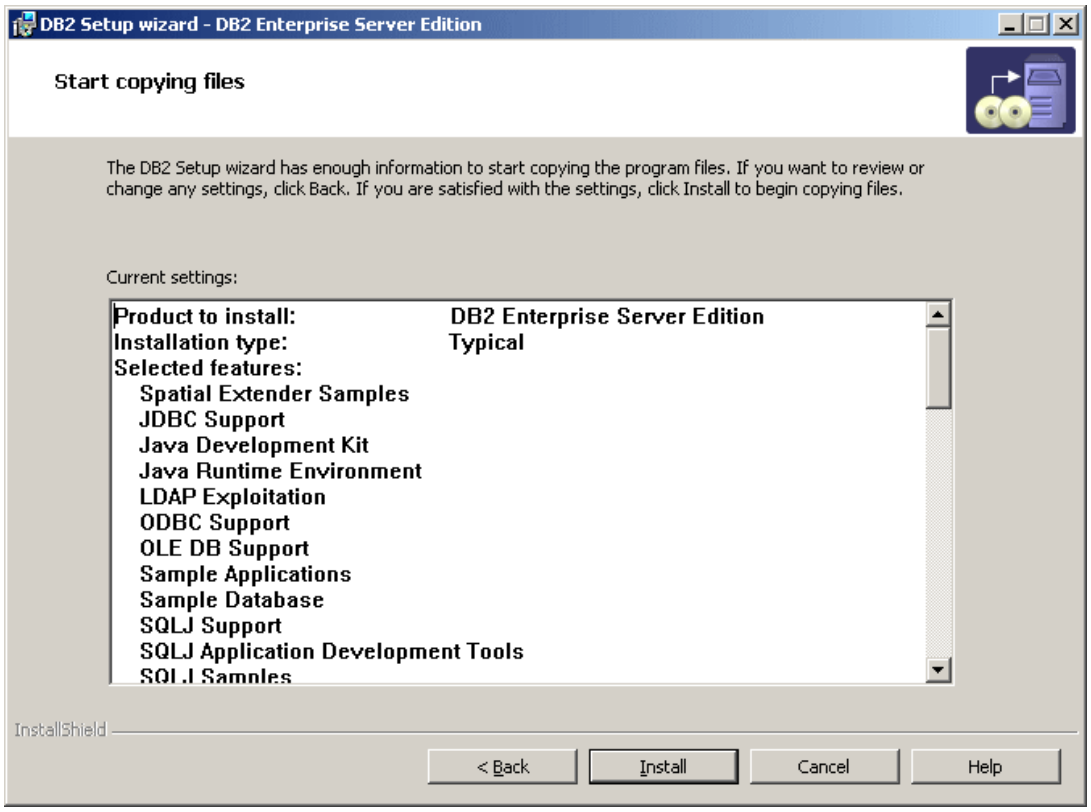

DB2 Setup wizard - DB2 Enterprise Server Edition
Start copying files
The DB2 Setup wizard has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Install to begin copying files.
Current settings:
Product to install: DB2 Enterprise Server Edition
Installation type: Typical
Selected features:
Spatial Extender Samples
JDBC Support
Java Development Kit
Java Runtime Environment
LDAP Exploitation
ODBC Support
OLE DB Support
Sample Applications
Sample Database
SQLJ Support
SQLJ Application Development Tools
SQLJ Samples
InstallShield
< Back
Install
Cancel
Help

Figure 6-13 Installation options summary

Downloaded from www.Manualslib.com manuals search engine

15. The installation may take a few minutes depending on the configuration of your server. When it is complete you are presented with the final window, shown in Figure 6-14. When you click **Finish** there may be additional dialogs called *First steps*, which you may safely close by clicking **Exit First Steps** in the bottom left corner.

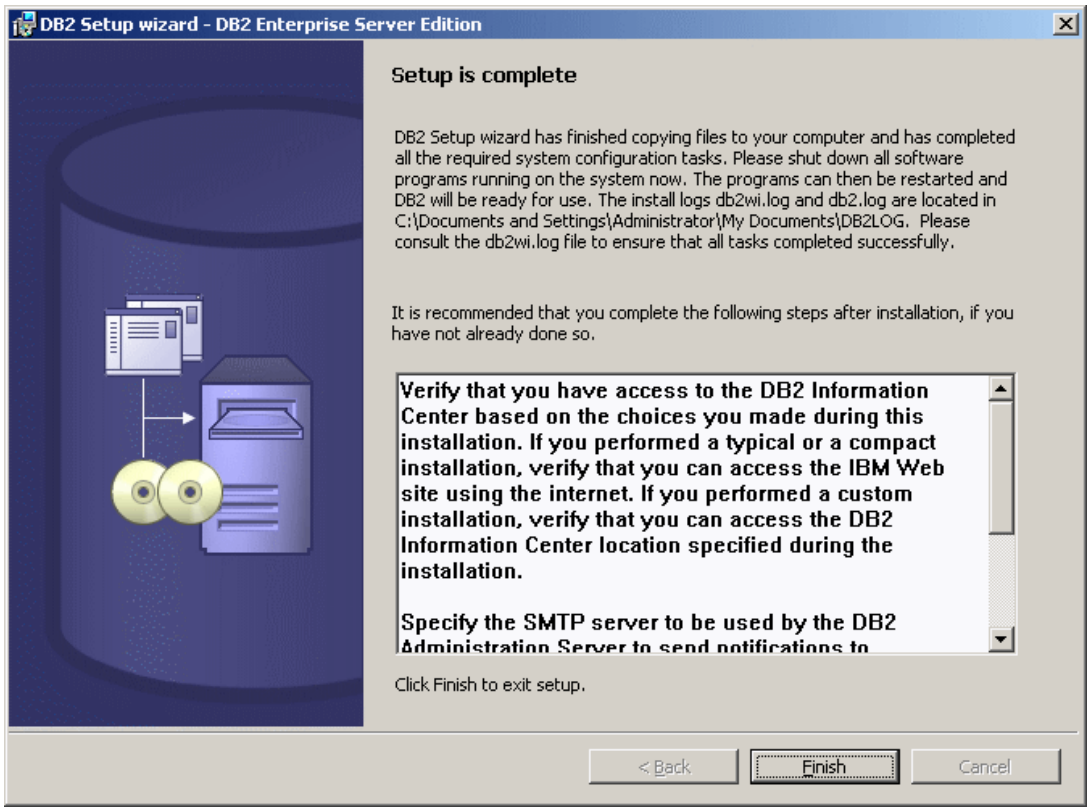

DB2 Setup wizard - DB2 Enterprise Server Edition
Setup is complete
DB2 Setup wizard has finished copying files to your computer and has completed all the required system configuration tasks. Please shut down all software programs running on the system now. The programs can then be restarted and DB2 will be ready for use. The install logs db2wi.log and db2.log are located in C:\Documents and Settings\Administrator\My Documents\DB2LOG. Please consult the db2wi.log file to ensure that all tasks completed successfully.
It is recommended that you complete the following steps after installation, if you have not already done so.
Verify that you have access to the DB2 Information Center based on the choices you made during this installation. If you performed a typical or a compact installation, verify that you can access the IBM Web site using the internet. If you performed a custom installation, verify that you can access the DB2 Information Center location specified during the installation.
Specify the SMTP server to be used by the DB2
Click Finish to exit setup.
< Back
Finish
Cancel

Figure 6-14 Installation completion window

This completes the installation of the DB2 database. You may proceed with installing the next components for the solution.

6.1.2 Installation of Tivoli Security Compliance Manager server

For the installation in our lab we used the refreshed base install of Tivoli Security Compliance Manager server, which comes with Version 5.1.1 (at the time of writing, it is also known as Fix Pack 30 to the Version 5.1.0).

1. To start the installation move to the folder where you have copied the installation files and run the scmserver_win32.exe file.

Downloaded from www.Manualslib.com manuals search engine

2. The usual language selection box is presented, as shown on Figure 6-15. Accept *English* and click **Next**.

Figure 6-15 Language selection dialog

3. Click **Next** on the Tivoli Security Compliance Manager Welcome window, which is presented next. There will be a license agreement window displayed, as shown in Figure 6-16. Accept the license and click **Next**.

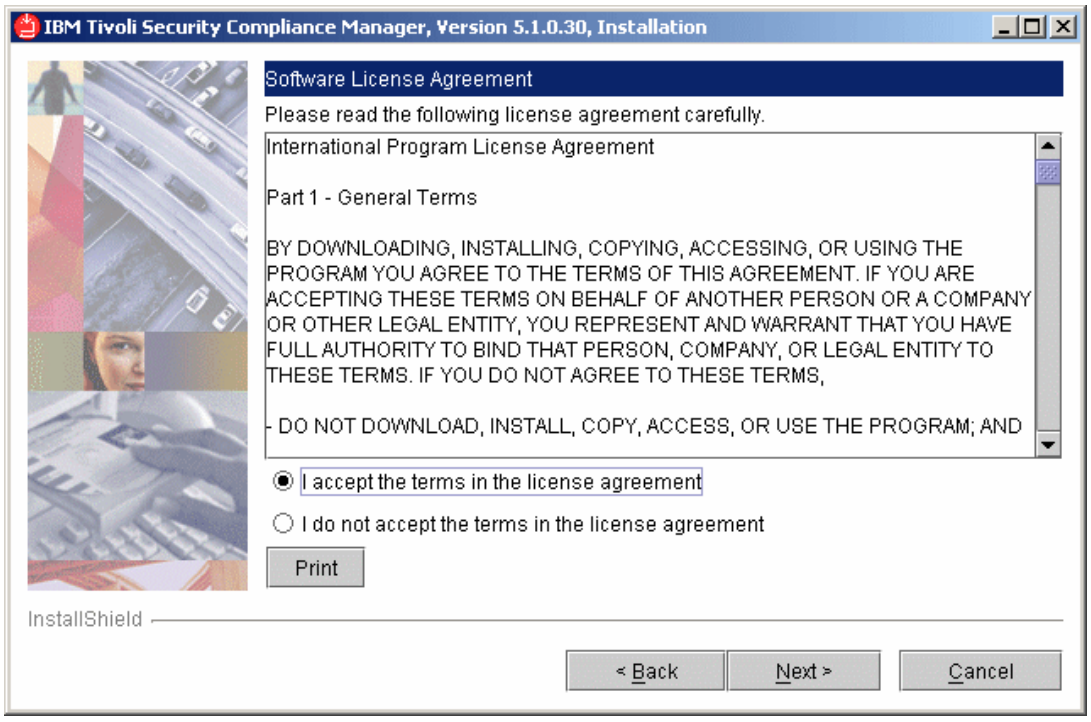

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

Figure 6-16 License agreement window

Downloaded from www.Manualslib.com manuals search engine

4. In the next window, shown in Figure 6-17, specify the destination directory for the Tivoli Security Compliance Manager installation. Accept the default, which is C:\Program Files\IBM\SCM, and click **Next**.

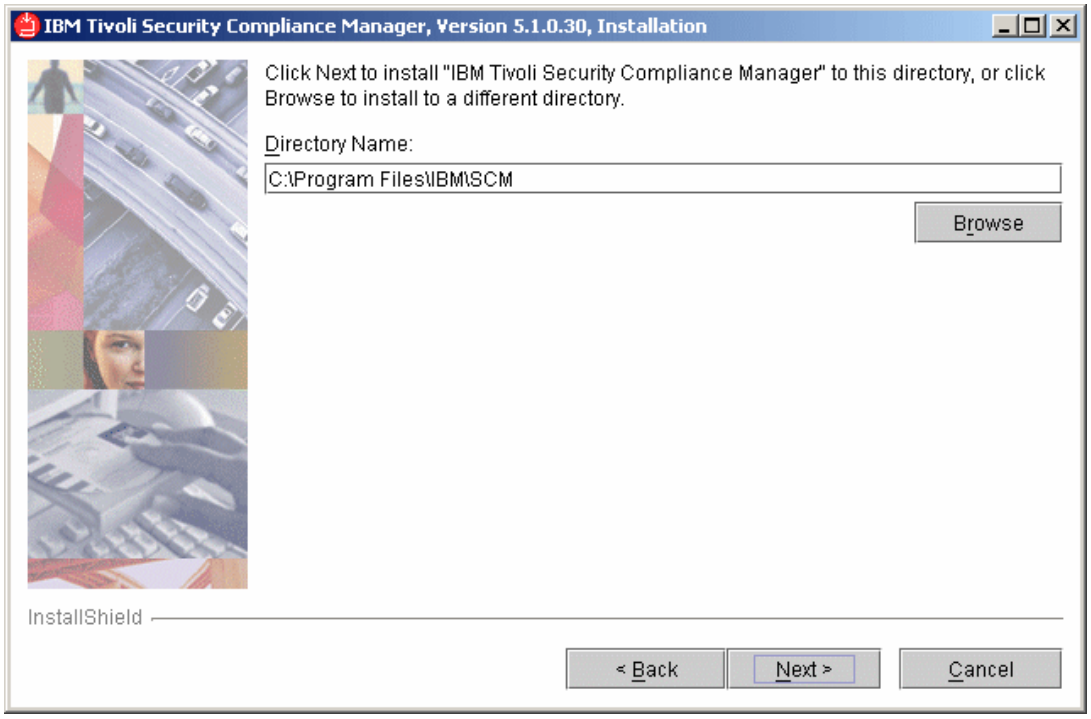

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Click Next to install "IBM Tivoli Security Compliance Manager" to this directory, or click Browse to install to a different directory.
Directory Name:
C:\Program Files\IBM\SCM
Browse
InstallShield
< Back
Next >
Cancel

Figure 6-17 Destination directory selection dialog

5. In the next window you may select what you want to have installed. There are three options available:

Administration Utilities When this option is selected the graphical user interface will be installed as well as the command line utilities for managing the server. This option is displayed during the installation on all supported operating systems. However, the graphical user interface can be installed only on Windows and Linux. The execution of this step on other operating systems will only deliver the command line utilities.

Server When this option is selected, all the components will be installed including the Administration Utilities and Database Configuration.

Database Configuration When this option is selected only the database configuration will be performed. This is useful if you decided to use a remote database for your

Downloaded from www.Manualslib.com manuals search engine

Tivoli Security Compliance Manager server installation. This is a recommended option in large scale deployments.

For this installation we must have all three components installed, so select the second option **Server**, as presented on Figure 6-18, and click **Next**.

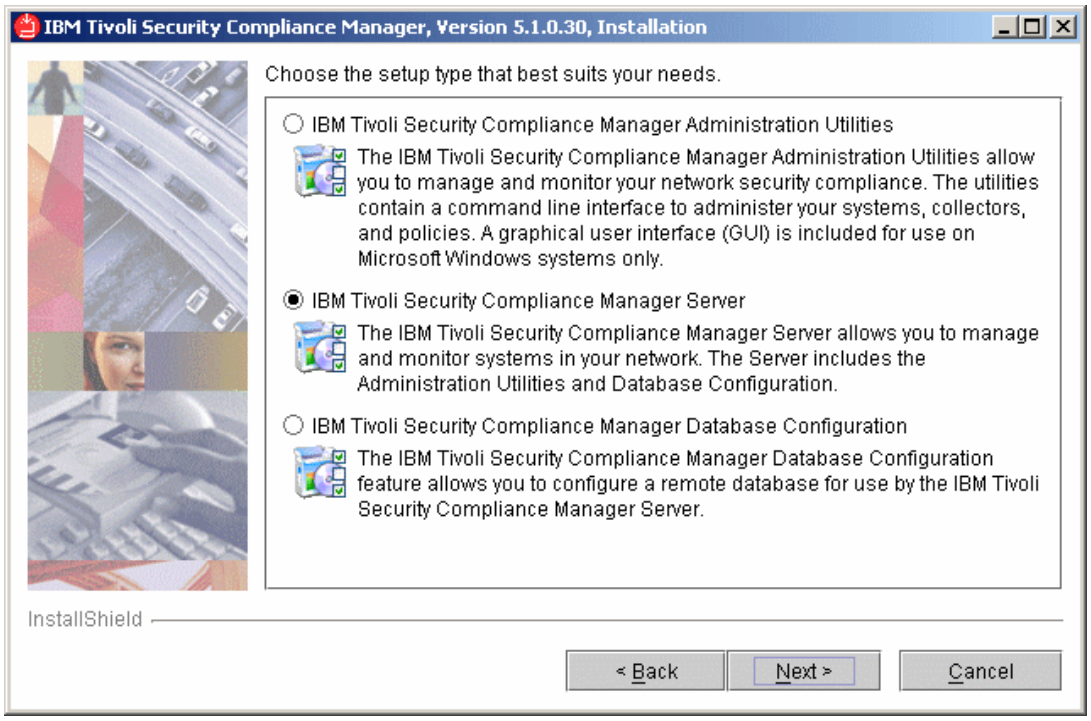

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Choose the setup type that best suits your needs.
IBM Tivoli Security Compliance Manager Administration Utilities
The IBM Tivoli Security Compliance Manager Administration Utilities allow you to manage and monitor your network security compliance. The utilities contain a command line interface to administer your systems, collectors, and policies. A graphical user interface (GUI) is included for use on Microsoft Windows systems only.
IBM Tivoli Security Compliance Manager Server
The IBM Tivoli Security Compliance Manager Server allows you to manage and monitor systems in your network. The Server includes the Administration Utilities and Database Configuration.
IBM Tivoli Security Compliance Manager Database Configuration
The IBM Tivoli Security Compliance Manager Database Configuration feature allows you to configure a remote database for use by the IBM Tivoli Security Compliance Manager Server.
InstallShield
< Back
Next >
Cancel

Figure 6-18 Setup type selection window

Downloaded from www.Manualslib.com manuals search engine

6. You are presented the e-mail Server configuration dialog, as shown in Figure 6-19. The Tivoli Security Compliance Manager server uses e-mails to notify the administrators of the violations found, as well as for distributing the reports. Specify the SMTP server name as well as the account the Tivoli Security Compliance Manager server will use to send the outgoing communication. If you do not have the SMTP server name available put any name there. You can easily change these values later in the server.ini configuration file. Then click **Next**.

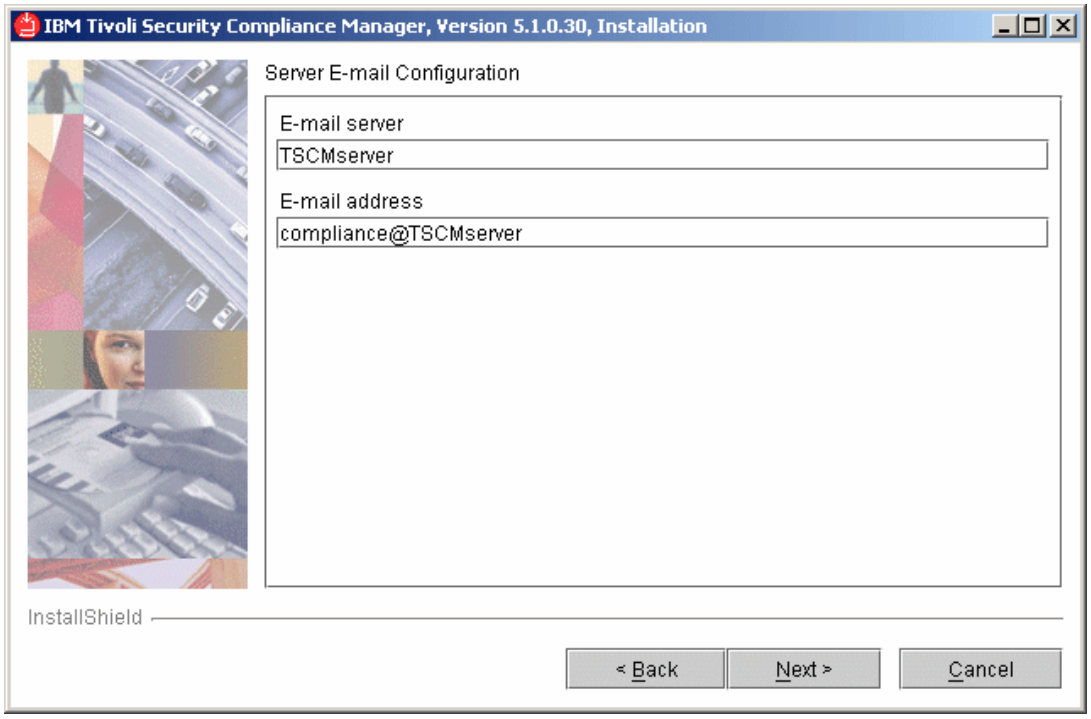


Figure 6-19 E-mail server configuration dialog

Downloaded from www.Manualslib.com manuals search engine

7. In the next window, shown on Figure 6-20, the installation wizard asks for the communication ports the server uses to communicate with the clients. We strongly recommend leaving the defaults. Click **Next**.

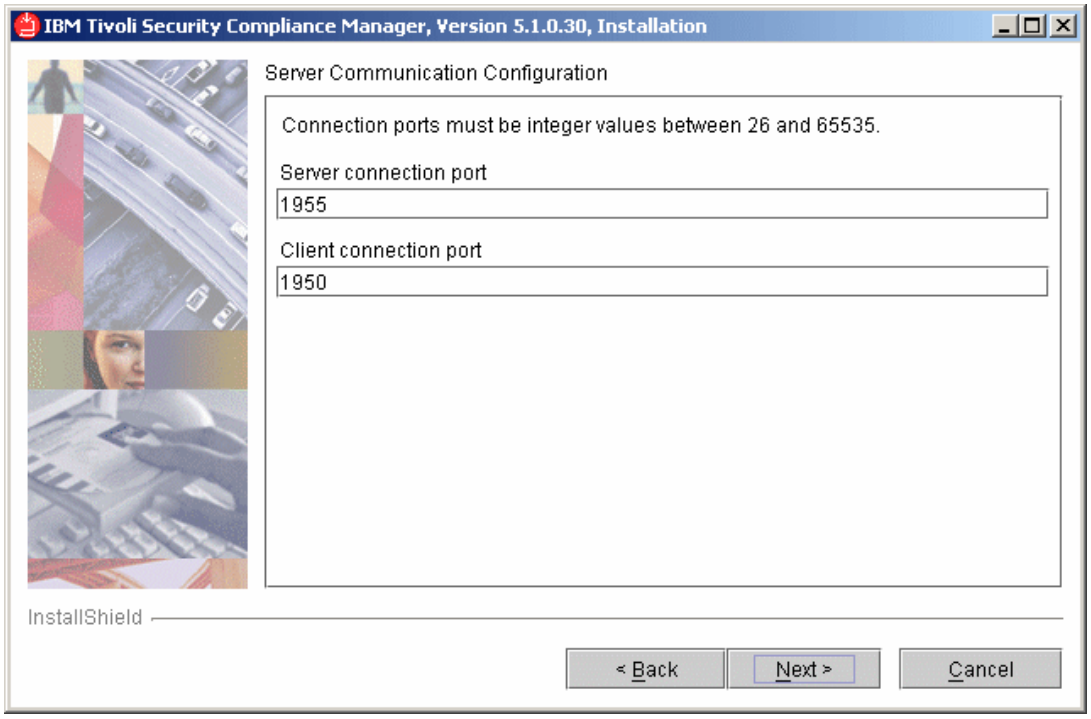


Figure 6-20 Server Communication Configuration window

Downloaded from www.Manualslib.com manuals search engine

8. The Server Security Configuration window is displayed, as shown in Figure 6-21. In the System name certificate field you must provide the system name that will be used to generate the self-signed certificate for the Tivoli Security Compliance Manager server. In the next four fields provide the passwords (and password confirmations) to access the keystore files generated during the installation. Then click **Next**.

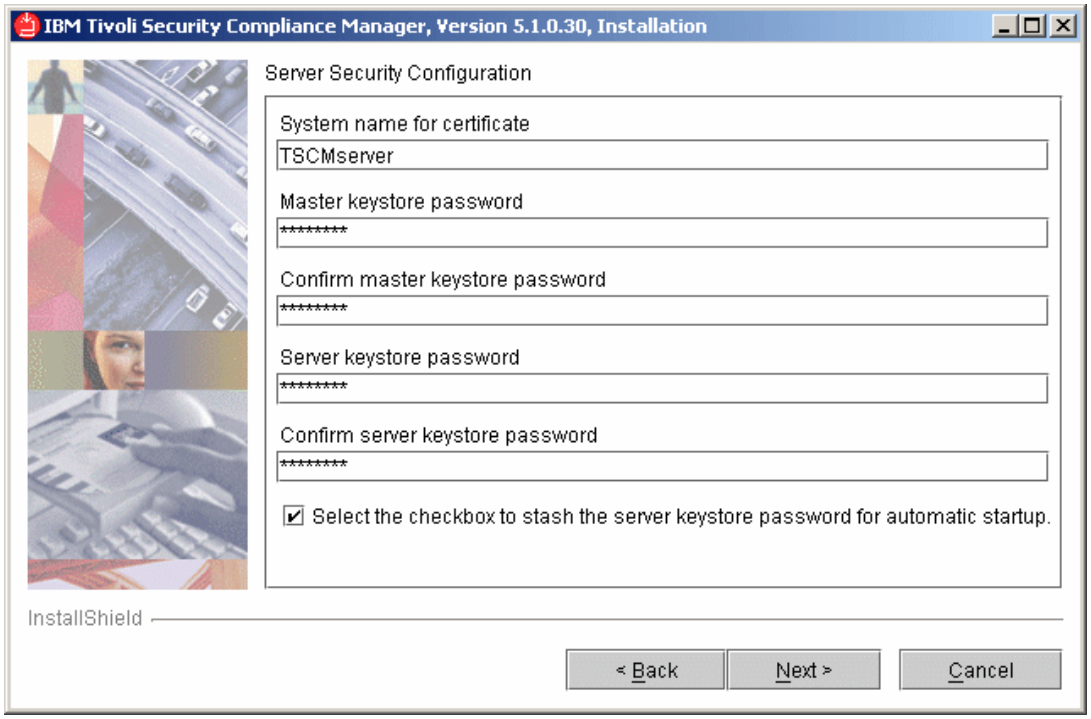


Figure 6-21 Server Security Configuration

Downloaded from www.Manualslib.com manuals search engine

9. In the next window, presented in Figure 6-22, select the location for your database. If you installed DB2 as described in 6.1.1, “Installation of DB2 database server” on page 126, select **The database is on the local system** option and click **Next**.

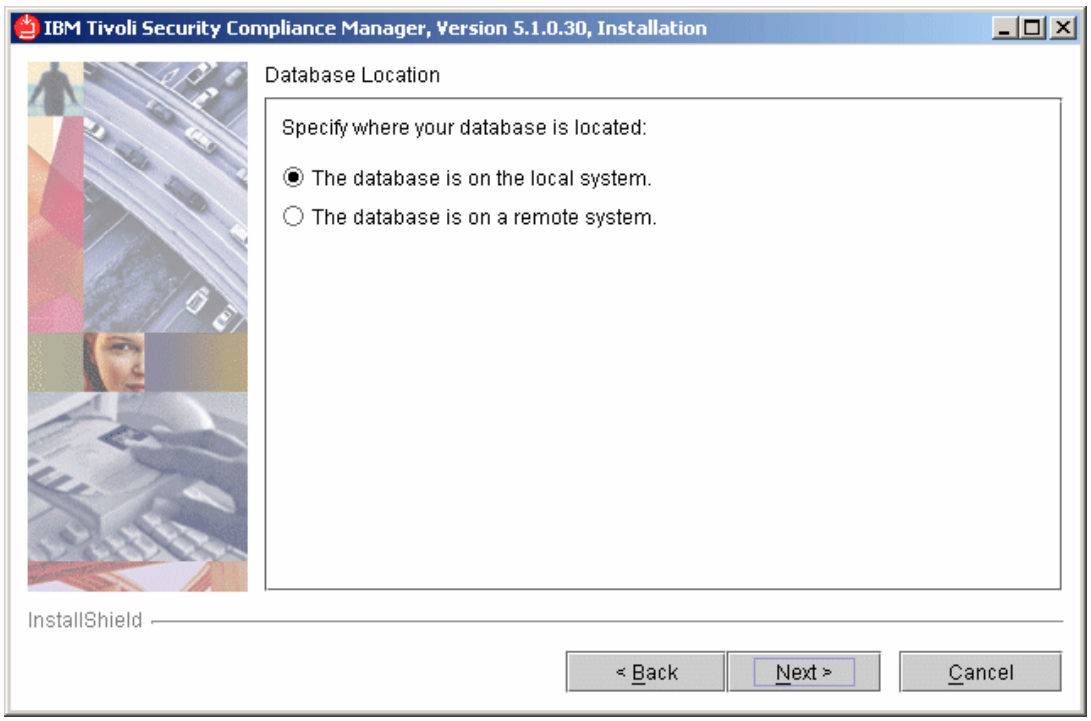

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Database Location
Specify where your database is located:
The database is on the local system.
The database is on a remote system.
InstallShield
< Back
Next >
Cancel

Figure 6-22 Database Location selection window

Downloaded from www.Manualslib.com manuals search engine

10. In the next dialog, provide the database configuration information, as shown in Figure 6-23. Enter the username and password for the DB2 administrator you have provided in step 9 on page 134. Leave the other fields with the default values and click **Next**.

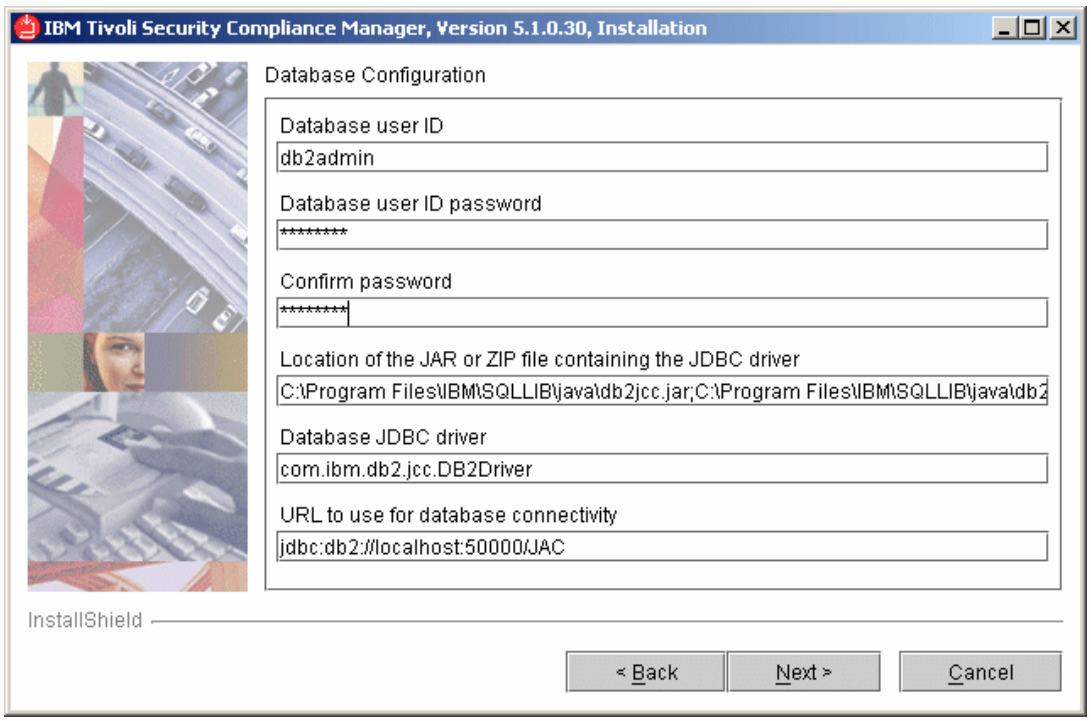


Figure 6-23 Database configuration information

Downloaded from www.Manualslib.com manuals search engine

11. In the next dialog, shown in Figure 6-24, you are asked whether the database should be created during this installation. Make sure that the check box is marked and click **Next**.

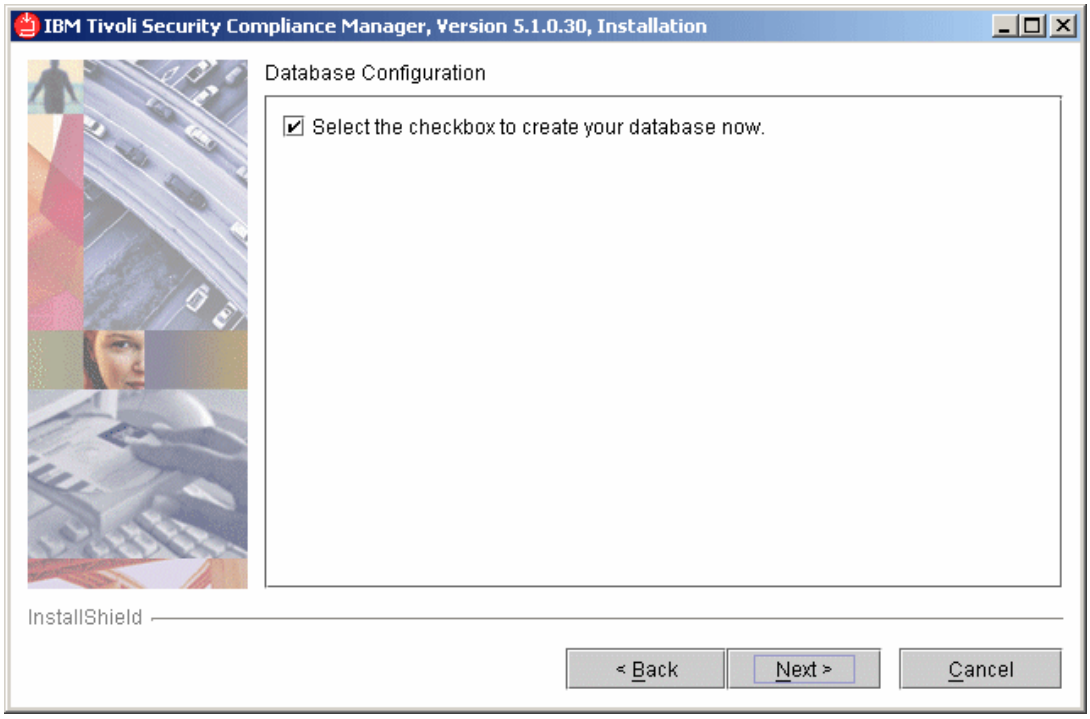

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Database Configuration
Select the checkbox to create your database now.
InstallShield
< Back
Next >
Cancel

Figure 6-24 Database creation choice window

Downloaded from www.Manualslib.com manuals search engine

12. The next dialog allows you to specify an administrator user ID and password for Tivoli Security Compliance Manager server, as shown in Figure 6-25. Use the name `admin` and enter a password of your choice. This user Id is created in the Tivoli Security Compliance Manager database and does not need to be a system account. Click **Next** to continue.

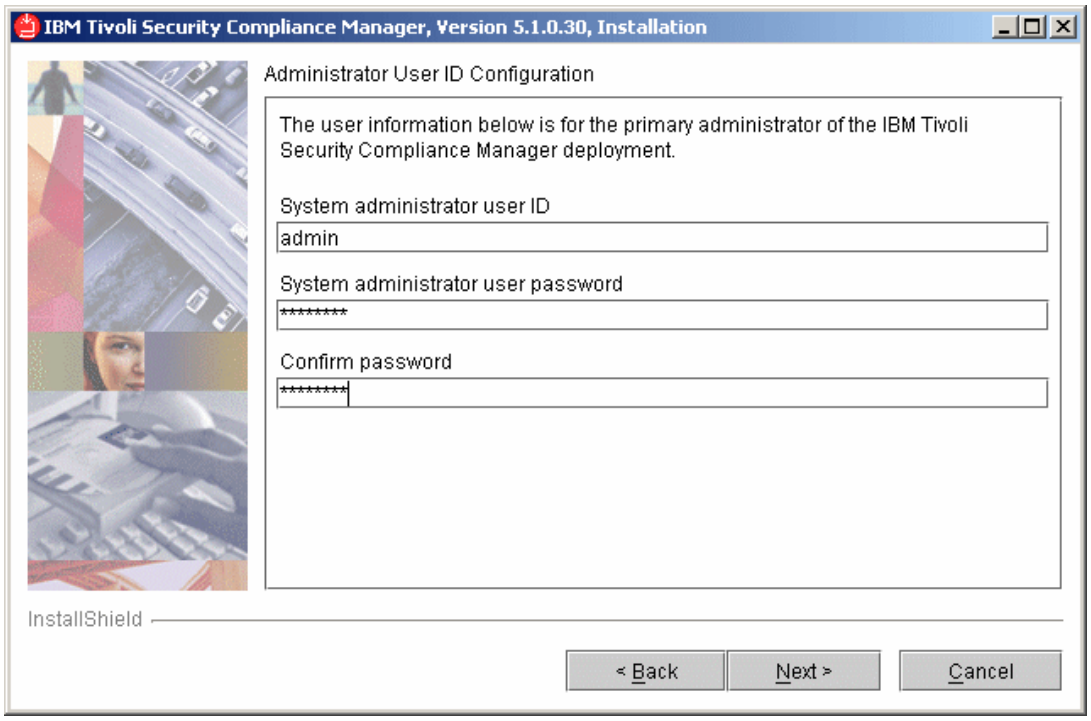

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Administrator User ID Configuration
The user information below is for the primary administrator of the IBM Tivoli Security Compliance Manager deployment.
System administrator user ID
admin
System administrator user password
****
Confirm password
****
InstallShield
< Back
Next >
Cancel

Figure 6-25 Administrator User ID Configuration window

Downloaded from www.Manualslib.com manuals search engine

13. Finally you are presented with the installation selection summary, as shown in Figure 6-26. Click **Next** to start the actual installation.

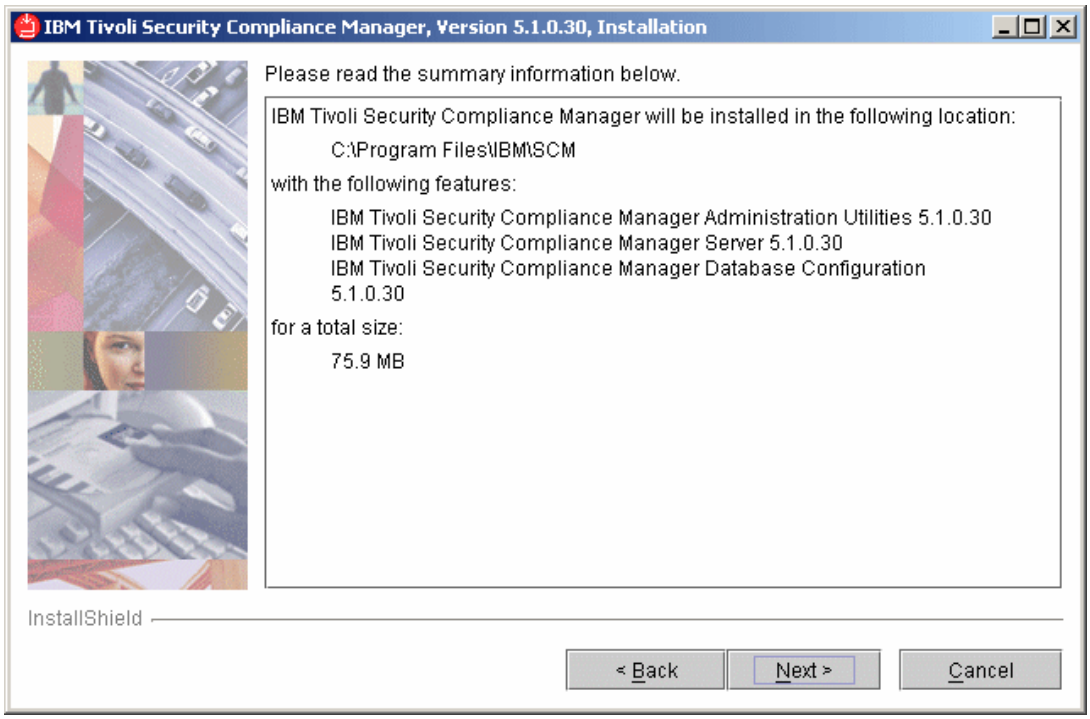

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Please read the summary information below.
IBM Tivoli Security Compliance Manager will be installed in the following location:
C:\Program Files\IBM\SCM
with the following features:
IBM Tivoli Security Compliance Manager Administration Utilities 5.1.0.30
IBM Tivoli Security Compliance Manager Server 5.1.0.30
IBM Tivoli Security Compliance Manager Database Configuration 5.1.0.30
for a total size:
75.9 MB
InstallShield
< Back
Next >
Cancel

Figure 6-26 Installation options summary window

Downloaded from www.Manualslib.com manuals search engine

14. The installation itself is very fast, but the database creation process may take a while. You may see the black command line window popping up listing the DB2 command execution results. *Do not* close this window. When the installation process is finished the last window is displayed, as shown in Figure 6-27. Click **Finish** to close the installation wizard.

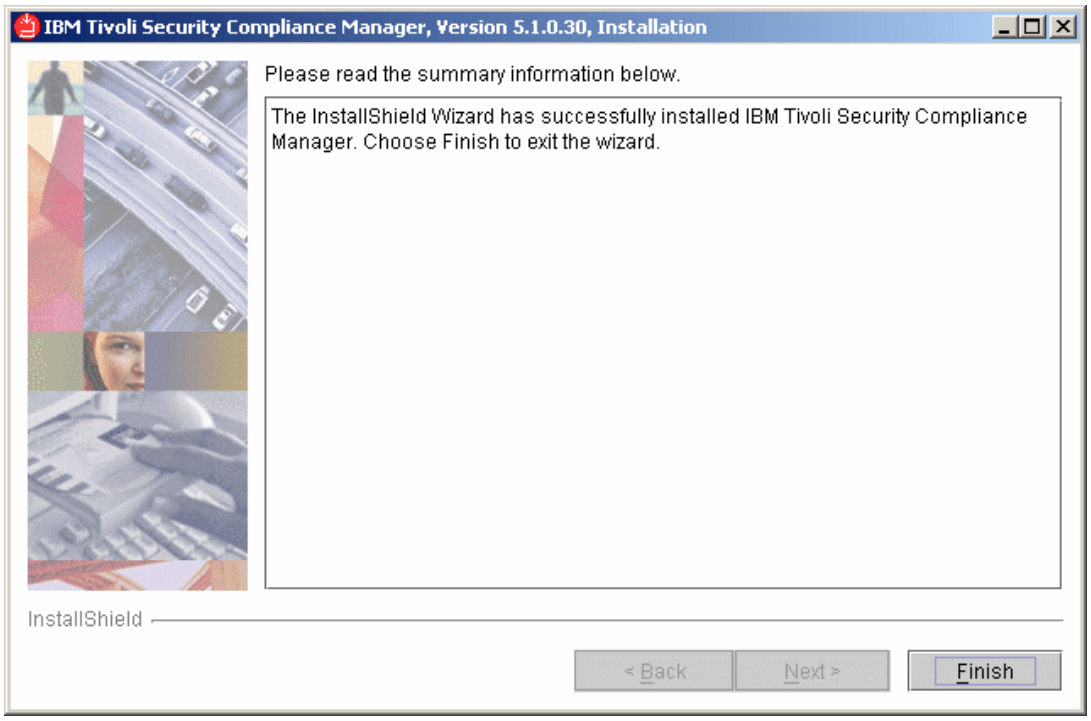

IBM Tivoli Security Compliance Manager, Version 5.1.0.30, Installation
Please read the summary information below.
The InstallShield Wizard has successfully installed IBM Tivoli Security Compliance Manager. Choose Finish to exit the wizard.
InstallShield
< Back
Next >
Finish

Figure 6-27 Installation result window

This concludes the Tivoli Security Compliance Manager server installation. You may proceed with the next components.

6.2 Configuration of the compliance policies

Since we have a Security Compliance Manager up and running we must set up the correct compliance policies to check for violations. For the purpose of this book we selected the following policies to be implemented and enforced:

- The antivirus software must be installed on the client workstation in the correct version, and it must be up-to-date with the virus signatures file and running. As an example we are using Symantec Antivirus software, but the solution can include rules for different antivirus software as well.

Downloaded from www.Manualslib.com manuals search engine

- The user password settings on the client workstation have to be following the policy, which means that the password must be at least eight characters in length and it must be renewed at least every 90 days.
- The appropriate operating system service pack level must be installed, which is Service Pack 4 for Windows 2000 and Service Pack 2 for Windows XP.
- Appropriate hotfixes must be applied. As an example we use the KB896423 and KB893756 hotfixes.
- The personal firewall must be running. We have used a ZoneAlarm personal firewall as the example. However, the rules can be easily modified to support other types as well.

In the sections below we describe the detailed processes of creating these policies. But first we want to introduce the posture collectors in more details.

6.2.1 Posture collectors

A posture collector collects compliance data the same way as a regular data collector. In most cases, one of the regular data collectors is included as part of the posture collector and the compliance data gathered is stored in the same database tables as the data collector. Posture collectors can be added to clients and client groups like regular collectors, and can run on an assigned schedule and return the collected data back to the Tivoli Security Compliance Manager server. Queries, reports, and policies can be defined and run to verify compliance using the data collected.

However, posture collectors differ from regular collectors in a number of substantial ways. First, posture collectors run automatically when the client is started or restarted. The information that is collected by the posture collectors is cached on the client system and can be used by the com.ibm.scm.nac.posture.PolicyCollector collector (or policy collector, for short) running on the client to make a security posture policy decision without contacting the Tivoli Security Compliance Manager server. The policy collector can run the posture collectors at any time to obtain the latest compliance data. Posture collectors also store posture information in an additional database table on the server, which indicates the security posture status of the client.

Posture items and posture elements

Every time a posture collector is run, a basic object called a posture item is created and cached. Each posture item consists of one or more posture elements that reflect the status of the data collection activity and the security posture checks performed by the posture collector. The PolicyCollector running on the client can directly access the posture items associated with the posture collectors and uses this information to make a security posture determination.

Downloaded from www.Manualslib.com manuals search engine

The status of a posture element can be one of the following:

PASS The data collection was successful, and the security posture of the selected item matches the required value.

FAIL The data collection was successful, but the detected value indicates that the client is noncompliant and remediation *must* be performed.

ERROR The data collection failed or an internal error occurred.

WARN The data collection was successful, but the detected value indicates that the client is not optimally compliant and remediation *is recommended*.

When the posture collector sends data to the Tivoli Security Compliance Manager server, the contents of the posture item are stored in the posture status table associated with the posture collector in the database.

Posture collector parameters

Posture collector parameters are generally required and indicate what data values should be checked, and what remediation should occur if a noncompliance is found. Parameters are of one of two types:

Operational Operational parameters are used to make a determination regarding a client system's security posture. For example, an operational parameter might indicate the required software version, or the required frequency of virus scans, or the maximum password age. If an operational parameter is not specified, the posture collector does not check the security posture represented by that parameter and indicates a warning in the corresponding posture element.

Workflow Workflow parameters are used for remediation purposes, and their names generally end with a _WF suffix. If a specific security posture check fails, the information provided by the workflow parameter is used to remedy the problem identified.

6.2.2 Policy collector

The com.ibm.scm.nac.posture.PolicyCollector.jar collector (or policy collector, for short) running on the client uses the information that is collected by the posture collectors to make a security posture policy decision without contacting the Tivoli Security Compliance Manager server. If a posture element returned by a posture collector indicates a violation, the policy collector can communicate that information, along with any associated remediation workflow information, to the

Downloaded from www.Manualslib.com manuals search engine

remediation subsystem, such as a Tivoli Configuration Manager. After the remediation has been performed, the remediation subsystem communicates to the policy collector to obtain updated status and, if necessary, perform additional remediation.

6.2.3 Installation of posture collectors

The compliance policies are defined on the Tivoli Security Compliance Manager server and are sets of rules verifying whether the data collected on the client meets the security policy criteria. However, it means that the data must first be collected using the appropriate collectors. When the Tivoli Security Compliance Manager is installed it contains no collectors or policies. The collectors must be installed first before any policies are defined. There are several ways to this, for example, installing them from the jar files posted on the Tivoli Security Compliance Manager support page or importing the already defined policy, which brings all the necessary collectors along and installs them on the server. We have chosen this second way.

As a starting point we used the sample policies provided with the IISSCN extension pack2 for Tivoli Configuration Manager.

To install them in your environment follow the steps below:

1. Create a temporary directory and extract the content of iisscn_extension_pack2.zip. Then go to the sample_policies subdirectory, where the following files should exist:
   - IISSCN_TCM_v2.00_win2000.pol
   - IISSCN_TCM_v2.00_winXP.pol
   - TCMCLI.pol
2. Start the Tivoli Security Compliance Manager Administration Console by selecting **Start** → **Tivoli Security Compliance Manager Administration Console** (or for Windows 2003 **Start** → **All programs** → **Tivoli Security Compliance Manager Administration Console**).

Downloaded from www.Manualslib.com manuals search engine

3. When the GUI pops up, as shown on Figure 6-28, log in with the credentials you specified during the installation, as described in step 12 on page 150 in the Installation of Tivoli Security Compliance Manager server procedure.

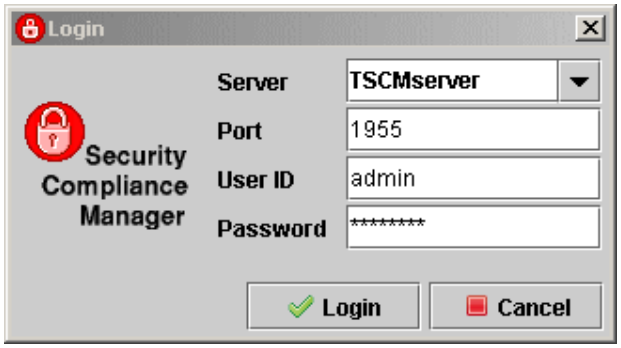


Figure 6-28 Tivoli Security Compliance Manager GUI login

4. If it is the first time you start the Administration Console you may be prompted to accept the new server identity, as shown on Figure 6-29. Just click **Accept Forever**.

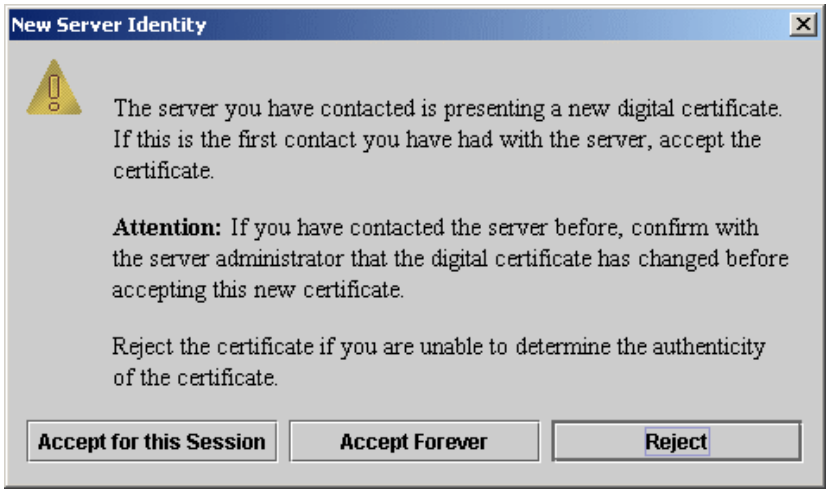

New Server Identity
The server you have contacted is presenting a new digital certificate. If this is the first contact you have had with the server, accept the certificate.
Attention: If you have contacted the server before, confirm with the server administrator that the digital certificate has changed before accepting this new certificate.
Reject the certificate if you are unable to determine the authenticity of the certificate.
Accept for this Session
Accept Forever
Reject

Figure 6-29 New Server Identity warning

Downloaded from www.Manualslib.com manuals search engine

5. You are presented with the default Message of the day window, which by default contains only the information about the Tivoli Security Compliance Manager version. Click **OK**. On the main Administrative Console window, as shown on Figure 6-30, switch to the **Policies** tab.

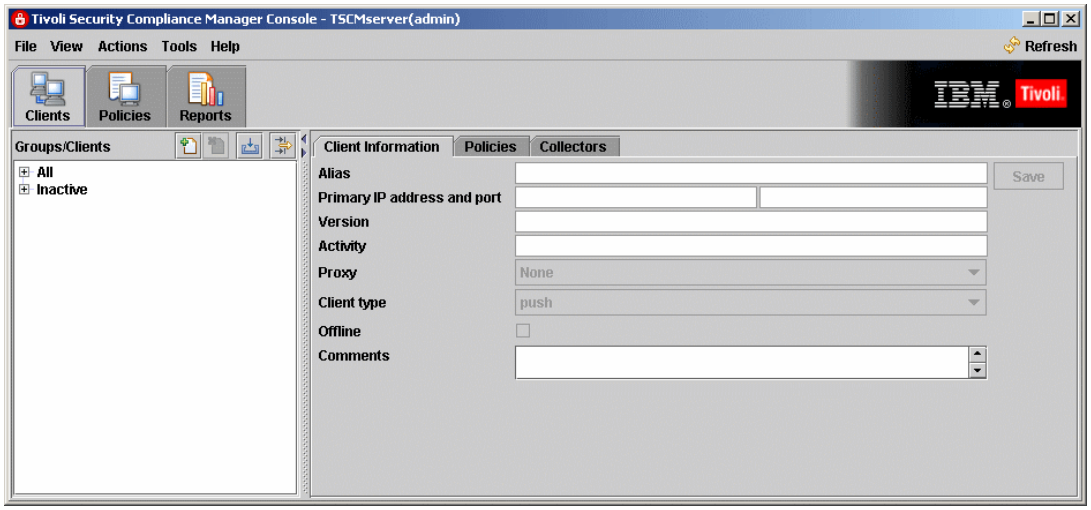


Figure 6-30 Tivoli Security Compliance Manager Administration Console

6. When you select menu **Action** → **Import Policy**, as shown in Figure 6-31, the file selection dialog is presented.

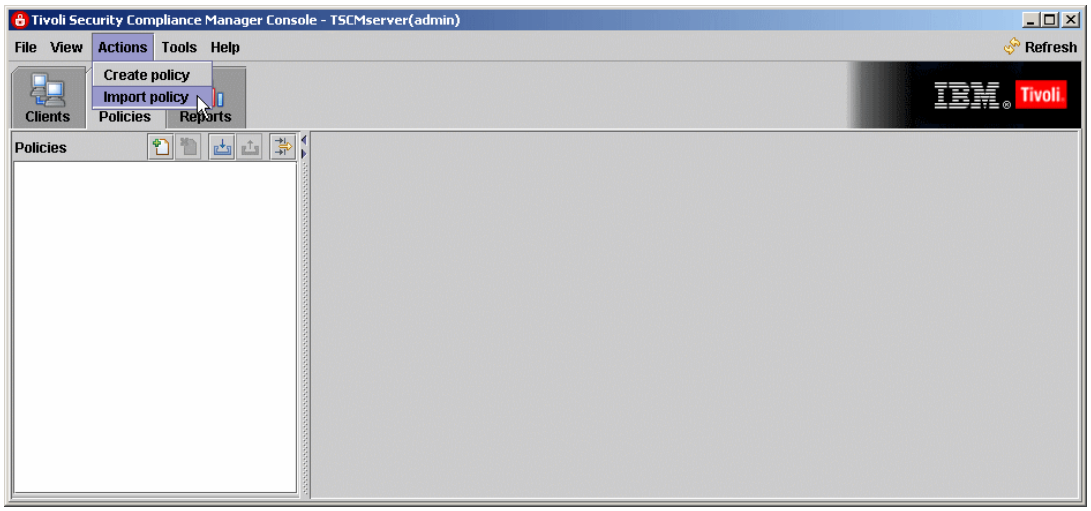


Figure 6-31 Import policy action menu

Downloaded from www.Manualslib.com manuals search engine

7. Navigate to the sample_polices directory created in step 1 and select the **TCMCLI.pol** file, as shown in Figure 6-32. Click **Import**.

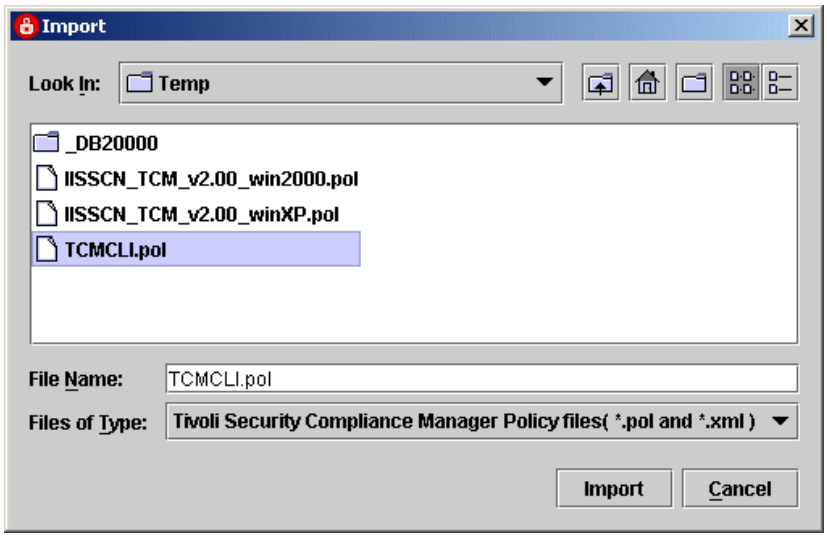


Figure 6-32 Import file selection dialog

8. In the next dialog, presented in Figure 6-33, you can change the default policy name. We recommend that you leave the default name unless you have this policy already imported and click **Next**.

Policy Name
Enter a new name for this policy. The name must not be the same as an existing installed policy.
TCMCLI
Cancel
Back
Next

Figure 6-33 Policy name dialog

Downloaded from www.Manualslib.com manuals search engine

9. In the next step the import wizard performs a validation of the signatures of the collectors included with the policy. When it is completed, as shown in Figure 6-34, click **Next**.

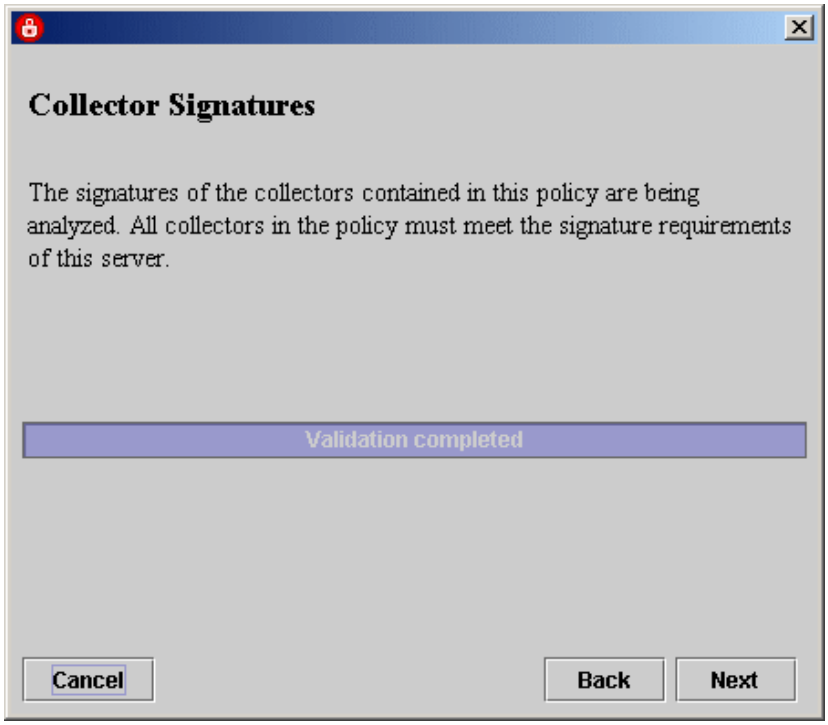

Collector Signatures
The signatures of the collectors contained in this policy are being analyzed. All collectors in the policy must meet the signature requirements of this server.
Validation completed
Cancel
Back
Next

Figure 6-34 Collectors signature validation

Downloaded from www.Manualslib.com manuals search engine

10. Now the actual policy installation is performed. Depending on the collectors you have already installed in your environment you may be asked if the existing collectors should be overwritten with the new ones included with the policy. If you are just following this book, there will be no warnings and you will be presented with the Policy Installation Summary, as shown in Figure 6-35. Click **Finish** to close the Import policy wizard.

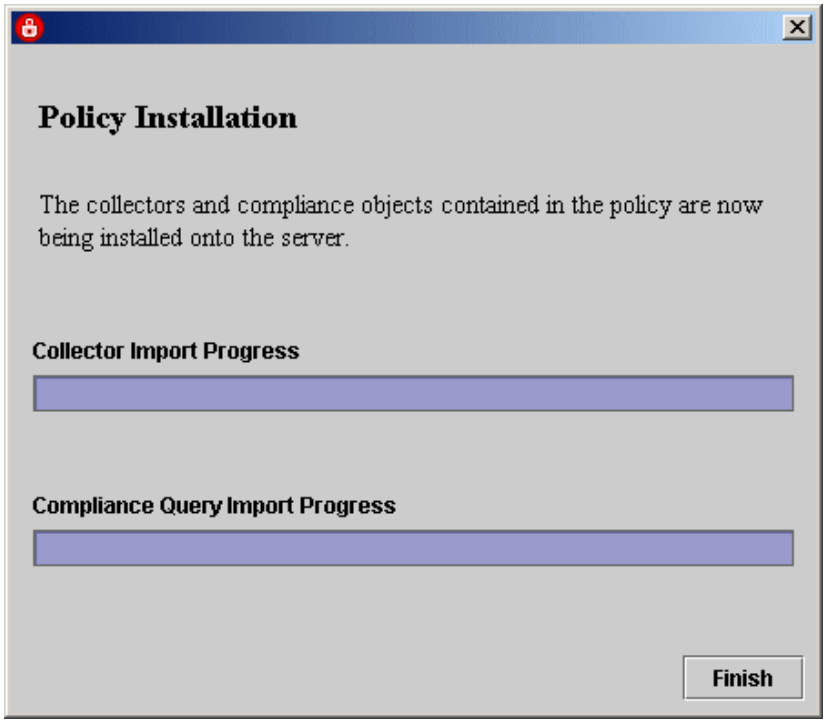

Policy Installation
The collectors and compliance objects contained in the policy are now being installed onto the server.
Collector Import Progress
Compliance Query Import Progress
Finish

Figure 6-35 Policy installation summary

Downloaded from www.Manualslib.com manuals search engine

11. After the wizard is closed you will see the imported policy in the Administrative Console, as shown in Figure 6-36.

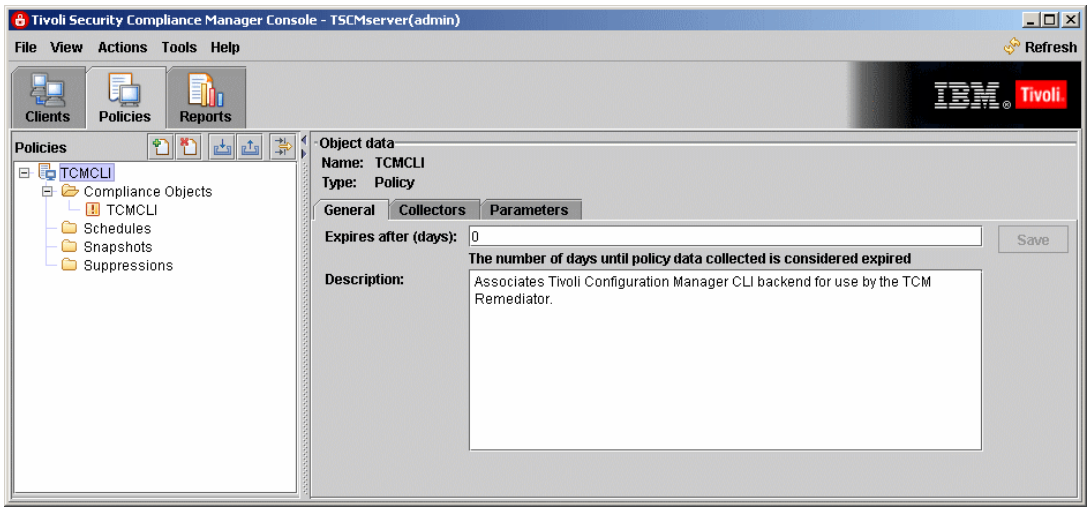


Figure 6-36 Compliance Policy view

To import the additional two sample policies named IISSCN_TCM_v2.00_winXP.pol and IISSCN_TCM_v2.00_win2000.pol, repeat steps 6 to 10, selecting the correct files accordingly.

6.2.4 Customization of compliance policies

To begin with the process of building customized polices for your environment we first need to explain the role of the policies imported in the previous section. There are a total of three policies, and two of them have names that are self-explanatory. The third policy, named TCMCLI, is the one that is special.

This policy must be assigned to every client that is supposed to use the auto remediation feature. This policy is not checking anything on the client. The only task of this policy is to distribute the correct level of Tivoli Configuration Manager stand-alone command-line utilities to the clients, which are then used to install the software package blocks downloaded from the Software Package Web Server during the remediation process.

Moving forward in the next section we describe the process of customizing the IISSCN_TCM_v2.00_winXP policy to meet the needs described in the first paragraph of 6.2, “Configuration of the compliance policies” on page 152.

We start with customizing the Symantec Antivirus compliance check. As opposed to the normal Tivoli Security Compliance Manager compliance checks, which are performed on the server based on the data collected from the clients and stored in the database, the policies used for Network Admission Control

Downloaded from www.Manualslib.com manuals search engine

must be evaluated on each client workstation. This is the reason why the appropriate values must be supplied as parameters for the NAC collectors rather then in the SQL query in the compliance object definition.

1. To start the customization open the Tivoli Security Compliance Manager Administration Console and log in as admin. Then move to the **Policies** tab and select the **IISSCN_TCM_v2.00_winXP** policy, as shown in Figure 6-37.

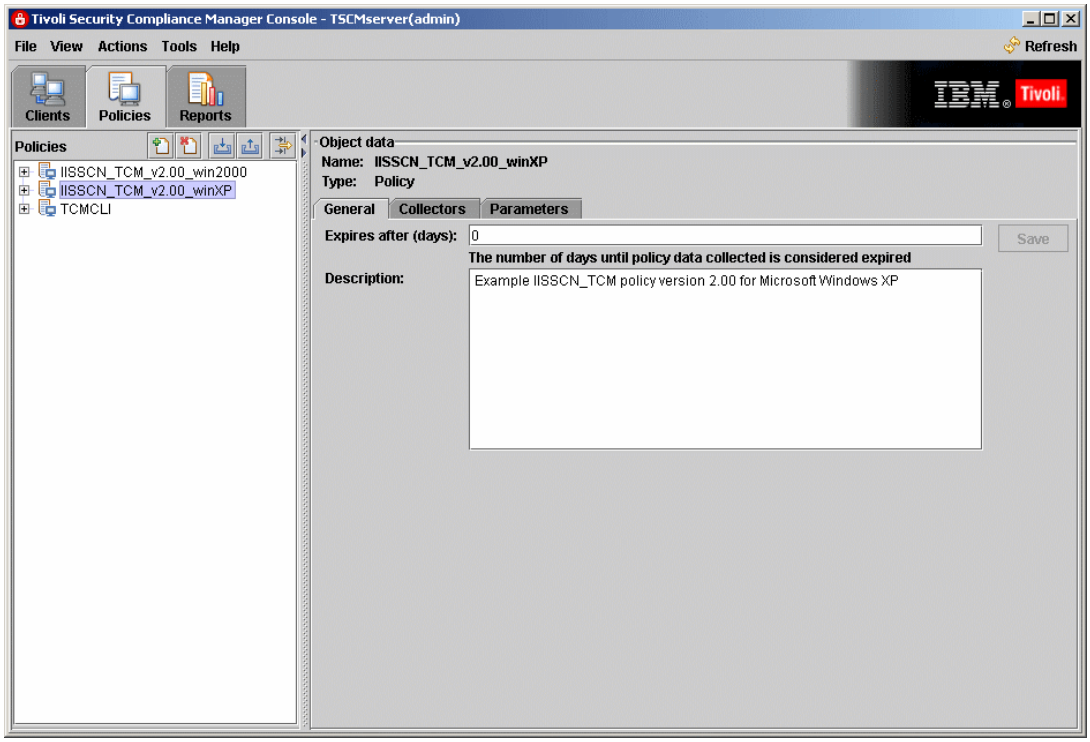


Figure 6-37 Policies view

Downloaded from www.Manualslib.com manuals search engine

2. In the right pane click the **Collectors** tab and select the Symantec Antivirus collector, as shown on Figure 6-38.

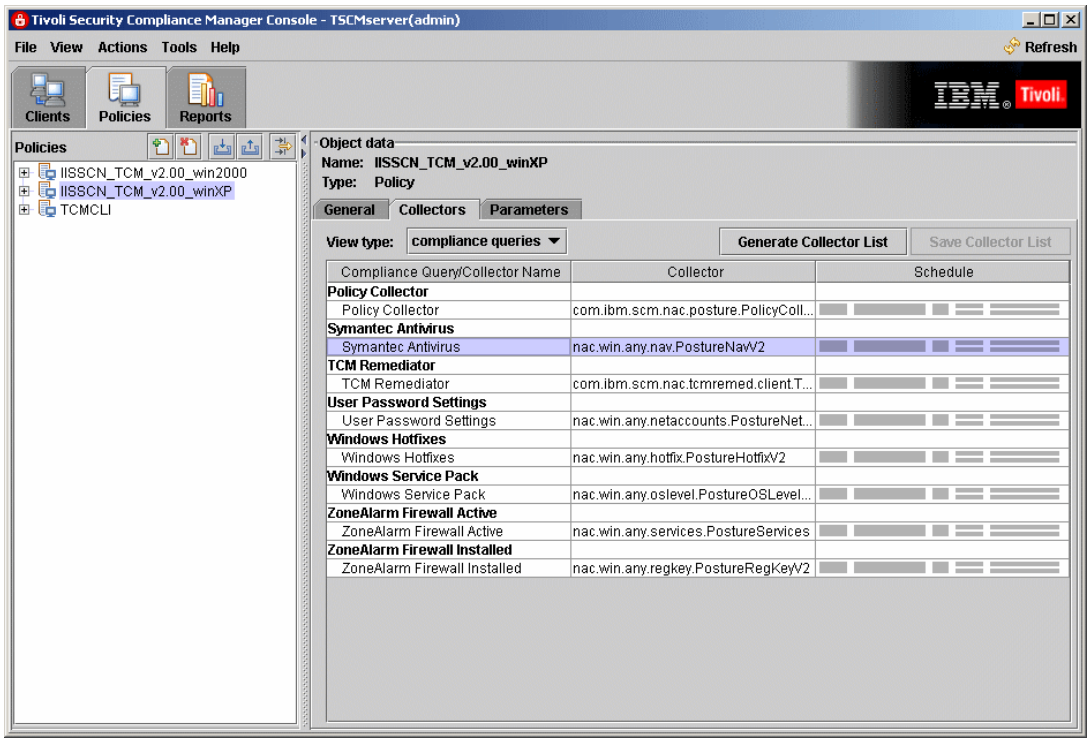


Figure 6-38 Collectors configuration view

3. The collector responsible for the Symantec Antivirus policy check is named nac.win.any.nav.PostureNavV2, and it is capable of checking three conditions regulated by the parameters specified on the Parameters dialog, shown in Figure 6-39. To open this window right-click the collector name and click **Edit collector parameters** from the pop-up menu.

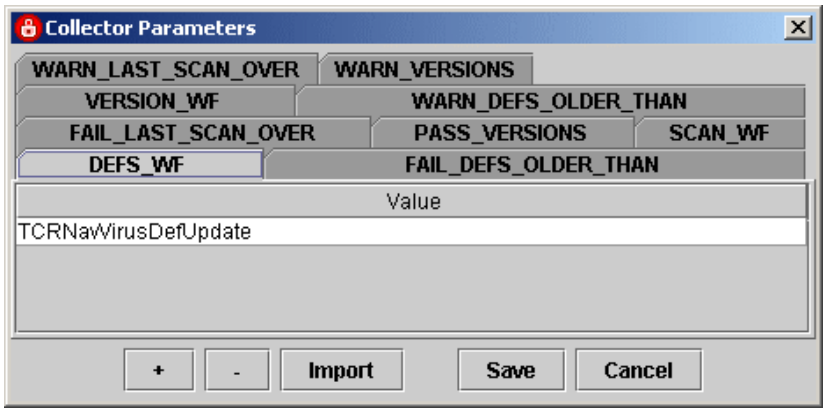


Figure 6-39 Parameters for Symantec Antivirus posture collector

Downloaded from www.Manualslib.com manuals search engine

The different conditions are:

- Version of the Symantec Antivirus Software
- Last scan date
- Age of the latest virus definition file

There are nine parameters regulating the behavior of the collector, as described in Table 6-1.

Table 6-1 Parameter information for nac.win.any.nav.PostureNavV2 collector

Parameter name	Parameter type	Description
PASS_VERSION	Operational	A list of acceptable Symantec/Norton Antivirus product versions. This list may consist of one or more entries.
WARN_VERSIONS	Operational	A list of Symantec/Norton Antivirus product versions that should be upgraded. This list may consist of one or more entries.
VERSION_WF	Workflow	Name of the workflow used for remediation if the software is not installed, or if the version installed must be upgraded.
FAIL_LAST_SCAN_OVER	Operational	An integer value used to indicate the allowable age, in hours, of the last scan before a failure is generated.
WARN_LAST_SCAN_OVER	Operational	An integer value used to indicate the allowable age, in hours, of the last scan before a warning is generated.
SCAN_WF	Workflow	Name of the workflow used for remediation if a scan must be performed.
FAIL_DEFS_OLDER_THAN	Operational	A time stamp in the format YYYY-MM-DD HH:MM:SS that the installed virus definitions must be more recent than to avoid generating a failure.

Downloaded from www.Manualslib.com manuals search engine

Parameter name	Parameter type	Description
WARN_DEFS_OLDER_THAN	Operational	A time stamp in the format YYYY-MM-DD HH:MM:SS that the installed virus definitions must be more recent than to avoid generating a warning.
DEFS_WF	Workflow	Name of the workflow used for remediation if the installed virus definitions need to be updated.

To adjust the parameters to your need modify the operational parameters, selecting the appropriate tabs. To add additional values to the parameter click the plus (+) sign. To remove a value click the minus (-) sign.

Do not change the default names of the remediation workflows.

When you are done editing click **Save**.

4. The next policy we customize is the one that regulates user password settings on the client workstation.

   Back at the list of collectors select and right-click the **User Password Settings** collector. Then click **Edit collector parameters**. The parameters for the collector nac.win.any.netaccounts.PostureNetAccountsV2 are displayed, as shown in Figure 6-40.

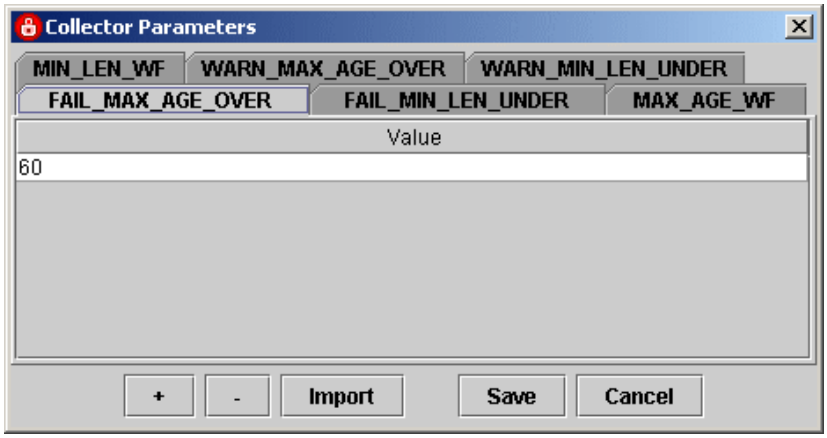


Figure 6-40 Parameters for User Password Settings posture collector

There are checks for:

- Minimum length of the user password
- Maximum allowed age of the user password

Downloaded from www.Manualslib.com manuals search engine

There are six parameters regulating the behavior of the collector, which are described in Table 6-2.

Table 6-2 Parameter information for nac.win.any.netaccounts.PostureNetAccountsV2

Parameter name	Parameter type	Description
WARN_MIN_LEN_UNDER	Operational	An integer value used to indicate the minimum allowable password length to avoid a warning.
FAIL_MIN_LEN_UNDER	Operational	An integer value used to indicate the minimum allowable password length to avoid a failure.
MIN_LEN_WF	Workflow	Name of the workflow used for remediation if the minimum password length is too short. This parameter should always be set when using the Tivoli Configuration Manager-based remediation solution.
WARN_MAX_AGE_OVER	Operational	An integer value used to indicate the maximum allowable password age, in days, to avoid a warning.
FAIL_MAX_AGE_OVER	Operational	An integer value used to indicate the maximum allowable password age, in days, to avoid a failure.
MAX_AGE_WF	Workflow	Name of the workflow used for remediation if maximum password age is too long. This parameter should always be set when using the Tivoli Configuration Manager-based remediation solution.

For the purpose of the book we require the following values to be checked:

- WARN_MIN_LEN_UNDER = 8
- FAIL_MIN_LEN_UNDER = 7
- WARN_MAX_AGE_OVER = 60
- FAIL_MAX_AGE_OVER = 90

To adjust the parameters to your need modify the operational parameters, selecting the appropriate tabs. These parameters accept only one integer value, so do not add multiple values and also do not change the default names of the remediation workflows.

Downloaded from www.Manualslib.com manuals search engine

When you are done editing click **Save**.

5. The next policy we customize is the one that checks for the appropriate operating system service pack level installed on the client workstation.

   Back at the list of the collectors right-click the **Windows Service Pack** collector. Then click **Edit collector parameters**, as shown in Figure 6-41.

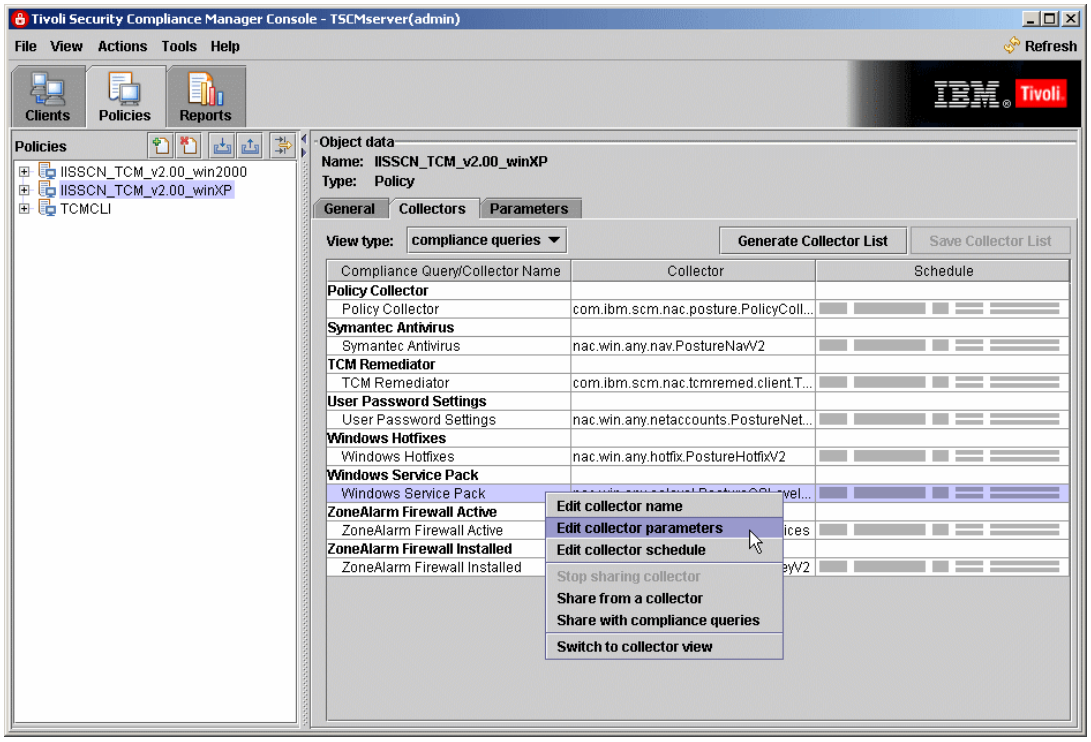


Figure 6-41 Editing collector parameters

Downloaded from www.Manualslib.com manuals search engine

6. The parameters for the collector nac.win.any.oslevel.PostureOSLevelV2 are displayed, as shown in Figure 6-42.

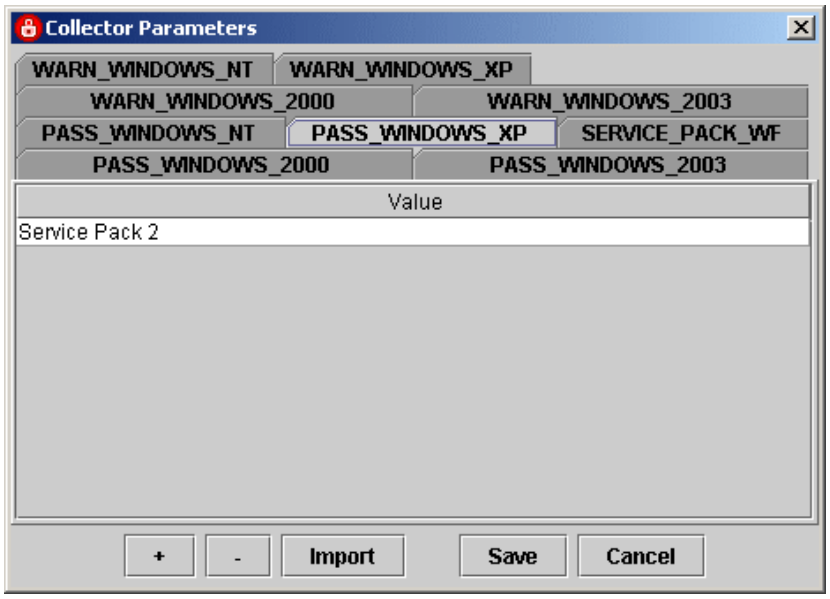


Figure 6-42 Parameters for Windows Service Pack collector

As you can see, this is a generic collector for all Windows versions. Since the policy we are editing is applied to Windows XP workstations, we only need to edit the two relevant parameters:

- WARN_WINDOWS_XP
- PASS_WINDOWS_XP.

The full list of parameters is described in Table 6-3.

Table 6-3 Parameter information for nac.win.any.oslevel.PostureOSLevelV2

Parameter name	Parameter type	Description
PASS_WINDOWS_NT	Operational	List of accepted service packs for the Microsoft Windows NT operating system
WARN_WINDOWS_NT	Operational	List of service packs that generate warnings for the Microsoft Windows NT operating system
PASS_WINDOWS_2000	Operational	List of accepted service packs for the Microsoft Windows 2000 operating system

Downloaded from www.Manualslib.com manuals search engine

Parameter name	Parameter type	Description
WARN_WINDOWS_2000	Operational	List of service packs that generate warnings for the Microsoft Windows 2000 operating system
PASS_WINDOWS_2003	Operational	List of accepted service packs for the Microsoft Windows 2003 operating system
WARN_WINDOWS_2003	Operational	List of service packs that generate warnings for the Microsoft Windows 2003 operating system
PASS_WINDOWS_XP	Operational	List of accepted service packs for the Microsoft Windows XP operating system
WARN_WINDOWS_XP	Operational	List of service packs that generate warnings for the Microsoft Windows XP operating system
SERVICE_PACK_WF	Workflow	Name of the workflow used for remediation if a service pack needs to be installed

The operational parameters listed above accept multiple values, so edit the appropriate parameters by selecting the proper tabs and adding all the versions accepted in your environment. To add additional values to the parameter click the plus (**+**) sign. To remove the value click the minus (**-**) sign.

Important: The paragraph below is different than for other collectors, so read carefully.

As opposed to the collectors described above, we *must change* the name of the workflow for collector nac.win.any.oslevel.PostureOSLevelV2. The solution was originally developed in Japan, so the default value for the SERVICE_PACK_WF parameter is TCRMSServicePackInstall_WinXpSp2Jp. Change this value to TCRMSServicePackInstallWinXPSP2.

When you are done editing click **Save**.

7. The next policy we customize is the one that checks for appropriate hotfixes installed on the client workstation.

Downloaded from www.Manualslib.com manuals search engine

Back at the list of the collectors right-click the **Windows Hotfixes** collector. Then click **Edit collector parameters**. The parameters for collector nac.win.any.hotfix.PostureHotfixV2 are displayed as shown in Figure 6-43.

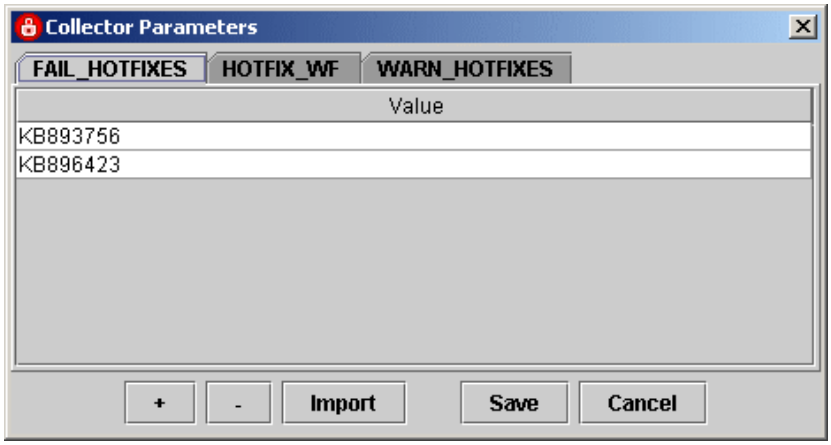


Figure 6-43 Parameters for Windows Hotfixes collector

This collector checks for the missing critical hofixes. The parameters are described in Table 6-4.

Table 6-4 Parameter information for nac.win.any.hotfix.PostureHotfixV2

Parameter name	Parameter type	Description
WARN_HOTFIXES	Operational	Parameter used to specify which Microsoft hotfixes are suggested. If a Microsoft hotfix in this list is missing, a WARN element will be generated.
FAIL_HOTFIXES	Operational	Parameter used to specify which Microsoft hotfixes are required. If a Microsoft hotfix in this list is missing, a FAIL element will be generated.
HOTFIX_WF	Workflow	Name of the workflow used for remediation if a suggested or required Microsoft hotfix is not installed.

The operational parameters listed above accept multiple values, so edit the appropriate parameters by selecting the proper tabs and adding all of the hotfixes that you require to be installed in your environment. To add additional values to the parameter click the plus sign. To remove the value click the minus sign.

Do not change the name of the workflow. When you are done editing click **Save**.

Downloaded from www.Manualslib.com manuals search engine

8. The next policy we configure checks whether the personal firewall is installed and running. Since we are using the generic posture collectors, this policy was implemented as two separate policies, one for checking the registry if the firewall is installed and the second to check the services if it is running.

   As an example we have chosen to check for the ZoneLabs firewall, but you can easily adjust these policies for any other personal firewall.

   First, at the collectors view select **ZoneAlarm Firewall Installed**, right-click, and click **Edit collector parameters** from the pop-up menu. You are presented with parameters for the generic nac.win.any.regkey.PostureRegKeyV2 collector, as shown in Figure 6-44. This is one of the most universal collectors, as it allows you to check the existence and value of any Windows registry key.

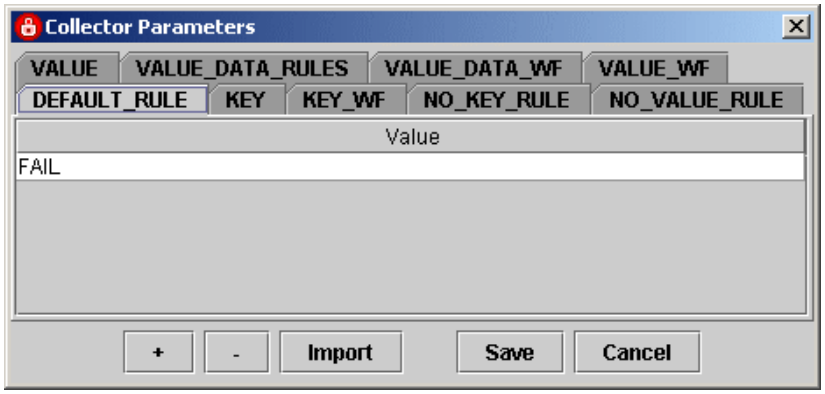


Figure 6-44 Parameters for RegKey collector

All the parameters for the nac.win.any.regkey.PostureRegKeyV2 collector are described in the Table 6-5.

Table 6-5 Parameter information for nac.win.any.regkey.PostureRegKeyV2

Parameter name	Parameter type	Description
KEY	Operational	Used to specify the name of the registry key to evaluate. Exactly one parameter value is required. If no parameter value is provided, no posture elements will be generated. If a parameter value is provided it will be used for the registry key existence check. If more than one parameter value is provided, only the first parameter value will be used.

Downloaded from www.Manualslib.com manuals search engine

Parameter name	Parameter type	Description
NO_KEY_RULE	Operational	Used to determine the status of the registry key existence check if the registry key specified in KEY is not found. No more than one parameter value should be provided. If more than one parameter value is provided, only the first parameter value will be used. The parameter value provided should be one of the following: PASS, WARN, or FAIL. If the parameter value is set to either WARN or FAIL, then the KEY_WF workflow is used. The required_values attribute of the workflow will be set to the parameter value of the KEY parameter. If the parameter value is set to something other than PASS, WARN or FAIL errors may occur.
VALUE	Operational	Used to specify which registry value of the key indicated by the KEY parameter should be evaluated. No more than one parameter value should be specified. If a parameter is provided it will be used for the registry value existence check. If no parameter value is provided, the only check run is the registry key existence check for the key specified in the KEY parameter. If more than one parameter value is provided, only the first parameter value will be used.
NO_VALUE_RULE	Operational	Used to determine the status of the registry value existence check if the registry key specified in the KEY parameter is found, but the registry value specified in the VALUE parameter is not. No more than one parameter value should be provided, in which case only the first parameter value will be used. The parameter value provided should be one of the following: PASS, WARN, or FAIL. If the parameter value is set to either WARN or FAIL, then the VALUE_WF workflow is used. The required_values attribute of the workflow will be set to the parameter value of the VALUE parameter. The workflow will also have the attribute key set to the parameter value of the KEY parameter. If no parameter value is provided and the registry value specified by the VALUE parameter does not exist for the key specified by the KEY parameter, then the parameter value of the DEFAULT_RULE parameter is used. If the DEFAULT_RULE parameter is not set, the registry value existence check defaults to PASS.

Downloaded from www.Manualslib.com manuals search engine

Parameter name	Parameter type	Description
VALUE_DATA_RULES	Operational	If the registry key specified in the KEY parameter and the registry value specified in the VALUE parameter both exist, then the contents of this parameter are used to determine the status of the registry value data check. The VALUE_DATA_RULES parameter should contain zero or more parameter values that make up the rules. Rules will be explained in more detail in a later section.
DEFAULT_RULE	Operational	Used by the collector to determine the status of various checks if a specific rule does not apply. No more than one parameter value should be provided. If more than one parameter value is provided, only the first parameter value will be used. The parameter value provided should be one of the following: PASS, WARN, or FAIL. If the parameter value is set to either WARN or FAIL, then a workflow may be used. If the parameter value is set to something other than PASS, WARN, or FAIL, errors may occur. If no parameter value is provided, this parameter defaults to PASS.
KEY_WF	Workflow	Contains the data attached to any workflow that is generated by the registry key existence check. Zero or more parameter values may be provided.
VALUE_WF	Workflow	Contains the data attached to any workflow that is generated by the registry value existence check. Zero or more parameter values may be provided.
VALUE_DATA_WF	Workflow	Contains the data attached to any workflow that is generated by the registry value data check. Zero or more parameter values may be provided.

The way this collector works depends on the data you have provided as parameters.

It first checks for the key existence if one is specified. Then it checks if the value is specified. Finally, if both are found, it verifies the rules specified in VALUE_DATA_RULES. There may be one or more rules specified. The construction of the rules is described below.

Downloaded from www.Manualslib.com manuals search engine

Rules

Rules are used to evaluate the detected registry value and determine the status of the registry value data element. All rules conform to simple rule grammar, and are composed of the following:

- A rule operator
- A rule value
- A rule result

A rule that logically evaluates to *true* is called a *matching rule*. A rule that evaluates to *false*, or cannot be evaluated, is called a *failing rule*. The rules listed in the VALUE_DATA_RULES parameter are evaluated sequentially from the top down until a matching rule is found, or the last rule is reached. If a matching rule is found, the status of the value data check is set to the rule's result and no more rules are evaluated. If all the rules are evaluated without finding a matching rule, then the status of the check is set to the contents of the DEFAULT_RULE parameter. If the DEFAULT_RULE parameter does not have a value, then the check is set to PASS.

Rule operators

Rules can be evaluated in either a numeric or a string context. The valid operators are listed in Table 6-6, with their meanings in both numeric and string contexts.

Table 6-6 Valid rule operators

Operator	String context	Numeric context
eq	Equal	N/D
ne	Not equal	N/D
=	N/D	Equal
!=	N/D	Not equal
<	N/D	Less then
<=	N/D	Less then or equal
>	N/D	Greater then
>=	N/D	Greater then or equal
<>	Not set	Not set
*	Is set	Is set

Downloaded from www.Manualslib.com manuals search engine

There are some limitations on numeric context evaluations. The collector initially receives all values from the underlying utilities as strings. For example, even though the registry type might be REG_DWORD and the value is set to 0x00000630, the collector will receive this value as the string 1584. Numeric checks are only run if both the value in the registry and the value in the rule can be converted to a 32-bit integer. All operators require a rule value for comparison except the two existence operators, * is set, and <> not set.

Rule results

All rules require a rule result. The rule result indicates what status should be set for the registry value data element. The rule result should be one of the following:

- PASS
- WARN
- FAIL

If the rule value is either WARN or FAIL, then the VALUE_DATA_WF workflow will be associated with the check. If a value was detected, the current_values attribute of the workflow will be set to the detected value. The workflow will also have the attribute key set to the parameter value of the KEY parameter and the attribute value set to the parameter value of the VALUE parameter. If the rule result is set to something other than PASS, WARN or FAIL errors may occur. If no rule result is provided, the parameter value of the DEFAULT_RULE parameter is used. If the DEFAULT_RULE parameter is not set, the Registry Value Data element defaults to PASS.

Rule format

The format of a rule is:

```
[operator][space][rule value][semicolon][{PASS | WARN | FAIL}]
```

For example:

```
= 100;PASS
```

Meaning that if the value of the key is equal numerically to 100, the status of the check is passed.

Below we discuss a few examples.

Checking for ZoneAlarm installation directory

If you want to check if the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm has a specific value InstallDirectory existing, provide the following parameters:

- KEY equal to HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm.

Downloaded from www.Manualslib.com manuals search engine

- VALUE equal to InstallDirectory.
- NO_KEY_RULE equal to FAIL.
- NO_VALUE_RULE equal to FAIL.
- Since you do not care about the actual value, but only of its existence, the VALUE_DATA_RULES must be set to:

  `*;PASS`
- If any of the three checks fail you want to have the same remediation workflow kicked off, so specify the same value for all three workflow parameters, for example, TCRZLSoftwareInstalled.

This example will pass only if the value InstallDirectory under key HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm is set. If it is not set, the TCRZLSoftwareInstalled workflow will be set for remediation with different parameters depending on which part of the check was missing.

Checking for Windows XP firewall forced off

In order to check whether the Windows XP Firewall is not forced off the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile must have the value EnableFirewall set to something else then 0 or not set at all. To conduct this check you must provide the following parameters:

- KEY equal to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile.
- VALUE equal to EnableFirewall.
- NO_KEY_RULE equal to PASS.
- NO_VALUE_RULE equal to PASS.
- VALUE_DATA_RULES need to be set to = 0;FAIL.
- DEFAULT_RULE equal to PASS.
- Since you need the remediation only in case the value exists and is set to 0 you must specify only one workflow parameter VALUE_DATA_WF to, for example, TCRFirewallForcedOff.

Downloaded from www.Manualslib.com manuals search engine

When you are done with editing the parameters for the nac.win.any.regkey.PostureRegKeyV2 collector click **Save**.

1. The second part of the firewall policy is meant to check whether the firewall service is running. This policy is checked using the generic nac.win.service.PostureServiceV2 collector. To open the parameter edition dialog shown in Figure 6-45, right-click the **ZoneAlarm Firewall Active** collector in the policy collector view and click **Edit collector parameters** from the pop-up menu.

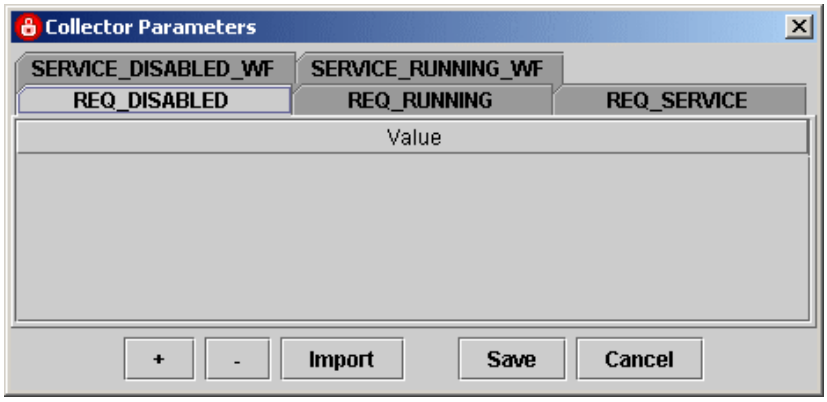


Figure 6-45 Parameters for Service collector

The nac.win.any.serice.ServicePostureV2 collector is able to check two conditions:

- If the service specified is running
- If the service specified is disabled

The parameters for the nac.win.any.serice.ServicePostureV2 collector are described in Table 6-7.

Table 6-7 Parameter information for nac.win.any.services.PostureServicesV2 collector

Parameter name	Parameter type	Description
REQ_SERVICE	Operational	One or more service names that will be checked. The values entered must exactly match the name of the service as it appears in the control panel Administrative Tools Services utility. This is a required parameter.

Downloaded from www.Manualslib.com manuals search engine

Parameter name	Parameter type	Description
REQ_RUNNING	Operational	A Boolean parameter used to indicate that the services listed in the REQ_SERVICE parameter must be running. A true value (1) indicates that the service must be running. A false value (0) indicates that the service must not be running. All other values are ignored.
SERVICE_RUNNING_WF	Workflow	The workflow used if the REQ_RUNNING check fails.
REQ_DISABLED	Operational	A Boolean parameter used to indicate that the services listed in the REQ_SERVICE parameter must have their startup mode set to disabled. A true value (1) indicates that the service must have its startup mode set to disabled. A false value (0) indicates the service must not have its startup mode set to disabled. All other values are ignored.
SERVICE_DISABLED_WF	Workflow	The workflow used if the REQ_DISABLED check fails.

To configure the policy with the right service name check it in the Services window on the client workstation and then enter the exact value on the REQ_SERVICE tab. In our lab we will check for `TrueVector Internet Monitor`, which is the name of the service for the ZoneAlarm personal firewall. As we want this service to be running the value of REQ_RUNNING must be set to 1.

Do not change the name of the workflow on the SERVICE_RUNNING_WF tab unless you have changed the service name (in case you are checking for a different firewall). In this second case you will need to change the name of the workflow on the Tivoli Configuration Manager server accordingly.

The ZoneAlarm firewall requires high security on the service access, so usually this service cannot be disabled by the end user, so we will not specify any values for the REQ_DISABLED and SERVICE_DISABLED_WF fields. The summary of the settings for this policy is presented below:

- SERVICE_REQ equal to TrueVector Internet Monitor
- REQ_RUNNING equal to 1

Downloaded from www.Manualslib.com manuals search engine

- SERVICE_RUNNING_WF equal to TCRZLSoftwareRunning
- REQ_DISABLED not set
- SERVICE_DISABLED_WF not set

When you are done editing click **Save**.

2. According to our security policy outlined in “Security compliance criteria” on page 100 we must add one more policy checking for the status of the Messenger service, which must be disabled. This service is installed by default on any Windows XP workstation, and our corporate security policy requires this service to be disabled. For that purpose we reuse the same collector type as for checking the ZoneAlarm service. However, this time we must specify the SERVICE_REQ, REQ_DISABLED and SERVICE_DISABLED_WF values. The sample policy we have imported does not include any check for the messenger service, so we must add this check.

   In the Tivoli Security Compliance Manager Administrator Console on the Policies view expand the **IISSCN_TCM_v2.00_winXP** policy and right-click the **ZoneAlarm Firewall Active** compliance query, as shown in Figure 6-46. Then click **Copy compliance query** from the pop-up menu.

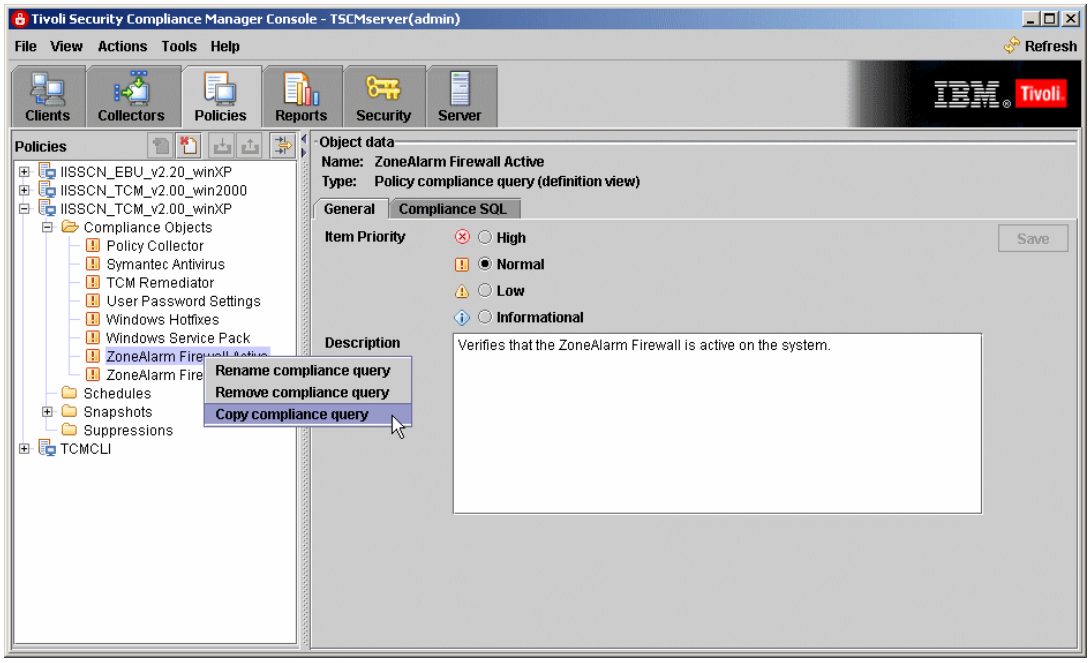


Figure 6-46 Copying an existing compliance query

Downloaded from www.Manualslib.com manuals search engine

The new dialog is presented, as shown in Figure 6-47. Select the destination policy for the copy process of the compliance query. Select **IISSCN_TCM_v2.00_winXP**, which is also the source for this compliance query, and click **OK**.

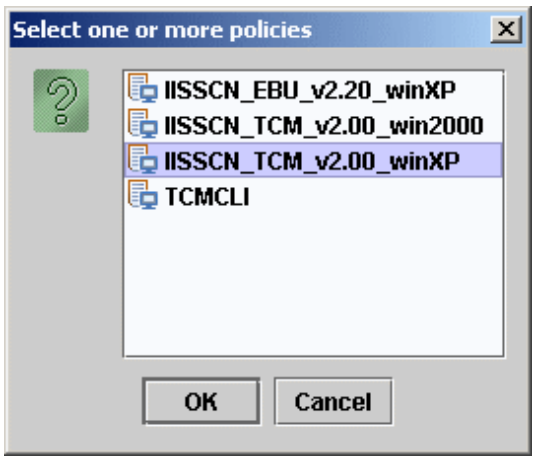


Figure 6-47 Destination policy selection dialog

Downloaded from www.Manualslib.com manuals search engine

There cannot be two compliance queries with the same name in one policy, so the copy of the compliance query is automatically renamed. It received an added _0 suffix. We must rename our new compliance query. Right-click the new **ZoneAlarm Firewall Active_0** compliance query and select **Rename compliance query**, as shown in Figure 6-48.

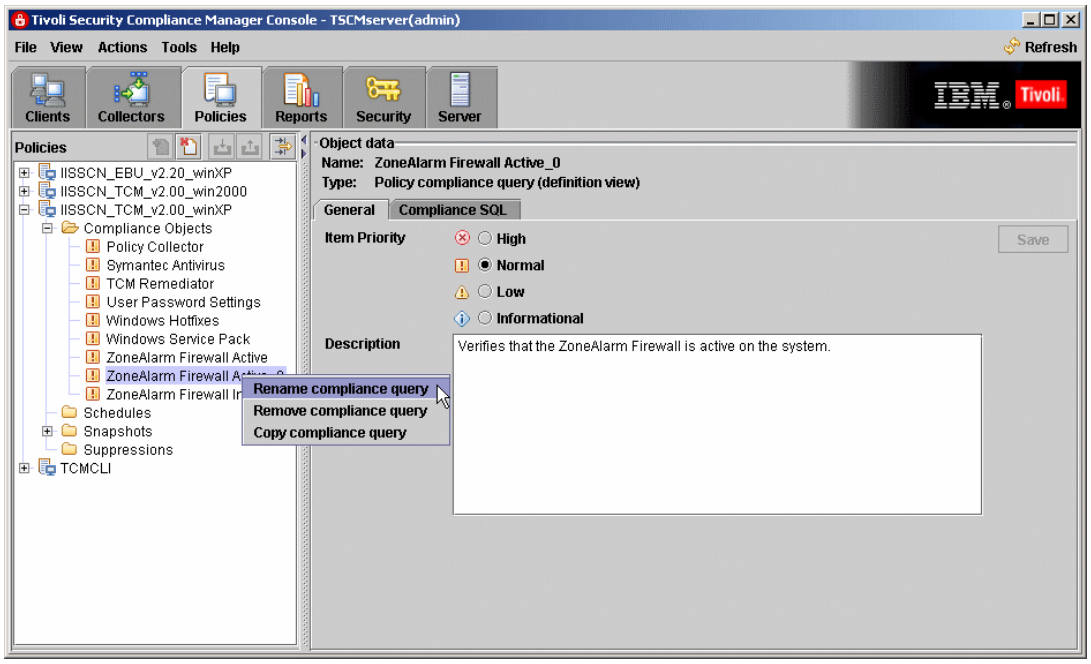


Figure 6-48 Renaming compliance query

Downloaded from www.Manualslib.com manuals search engine

In the following dialog modify the name value to `Messenger Service Disabled` and click **OK**. Then, in the right pane, modify the description of the compliance query, as shown on Figure 6-49, and click the **Save** button on the right.

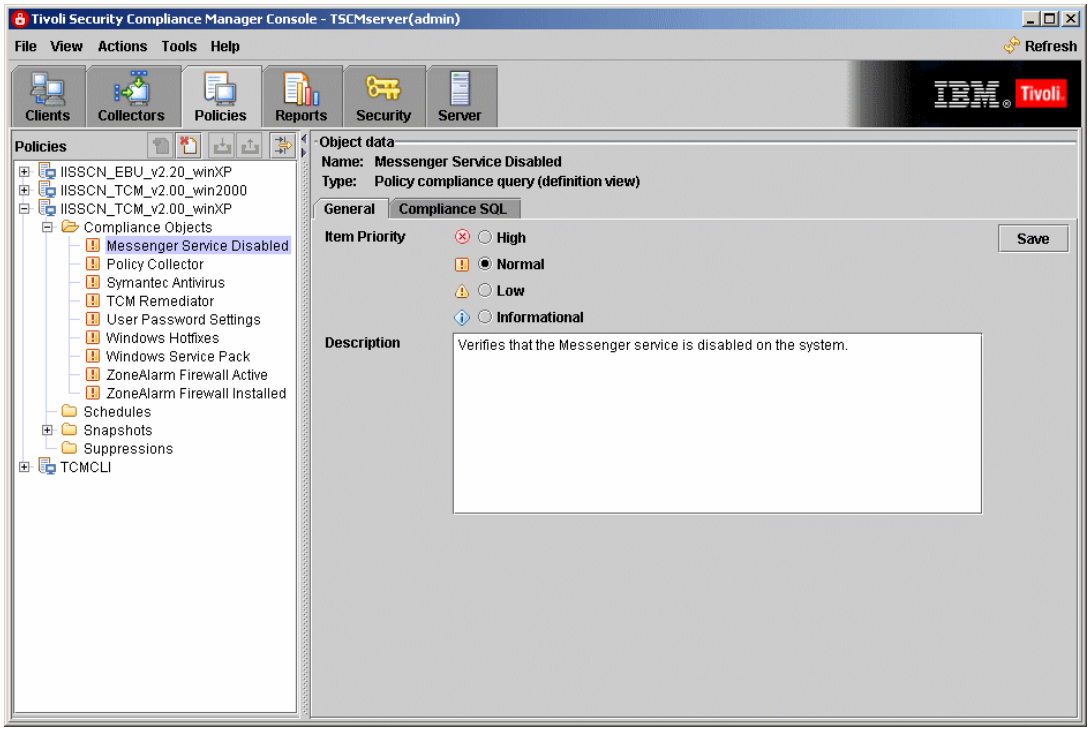


Figure 6-49 Compliance query description modification

Downloaded from www.Manualslib.com manuals search engine

Next select the **Compliance SQL** tab on the right pane and modify the violation message generated by the compliance check, as shown in Figure 6-50. There is no need to change the SQL compliance query itself, as it does not refer to any values other than the number of violations, which is generic for all services. When done with the editing click **Save**.

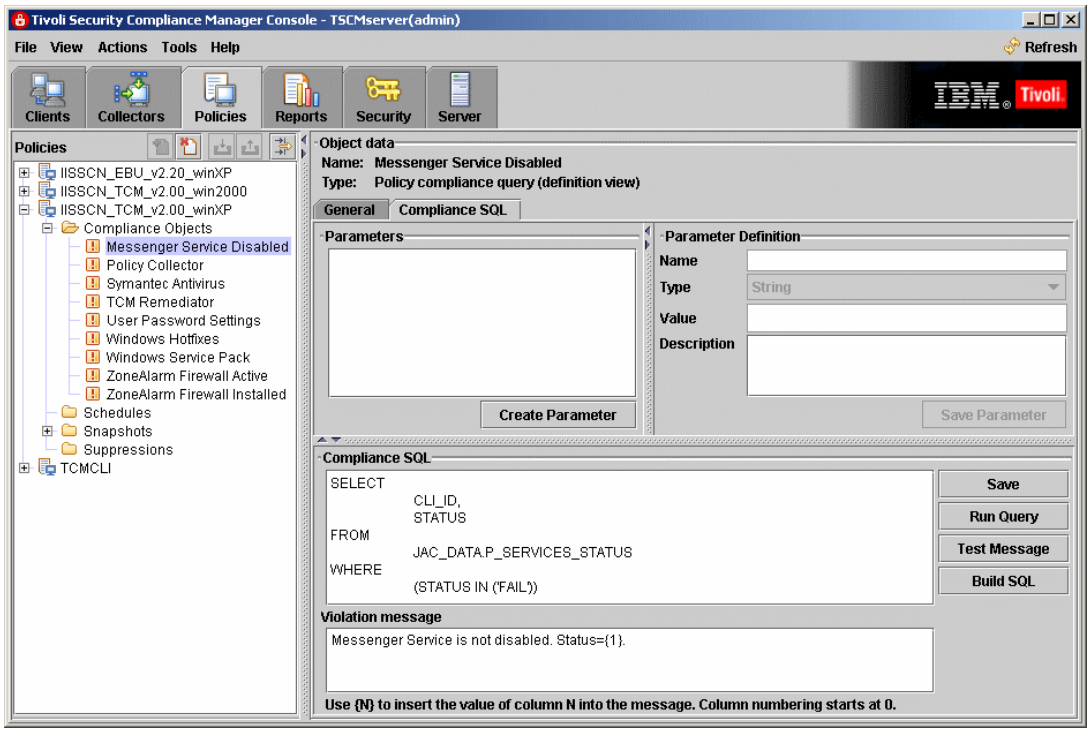


Figure 6-50 Violation message modification

Next we modify the collector parameters for the Messenger Service Disabled compliance query. Select the **IISSCN_TCM_v2.00_winXP** policy in the left pane and then click the **Collectors** tab for this policy in the left pane. Click the **Generate Collector List** to refresh the view. You may notice the new lines that are shown for the Messenger Service Disabled compliance query, but having the ZoneAlarm Firewall Active name underneath. This is because, by default, if there are more queries using data from one type of the collector, they are using only one instance of the collector. Since we must specify a separate set of parameters we want to have a separate instance of the

Downloaded from www.Manualslib.com manuals search engine

collector as well. Right-click the **ZoneAlarm Firewall Active** name under Messenger Service Disabled and click **Stop sharing collector item** from the pop-up menu, as shown in Figure 6-51.

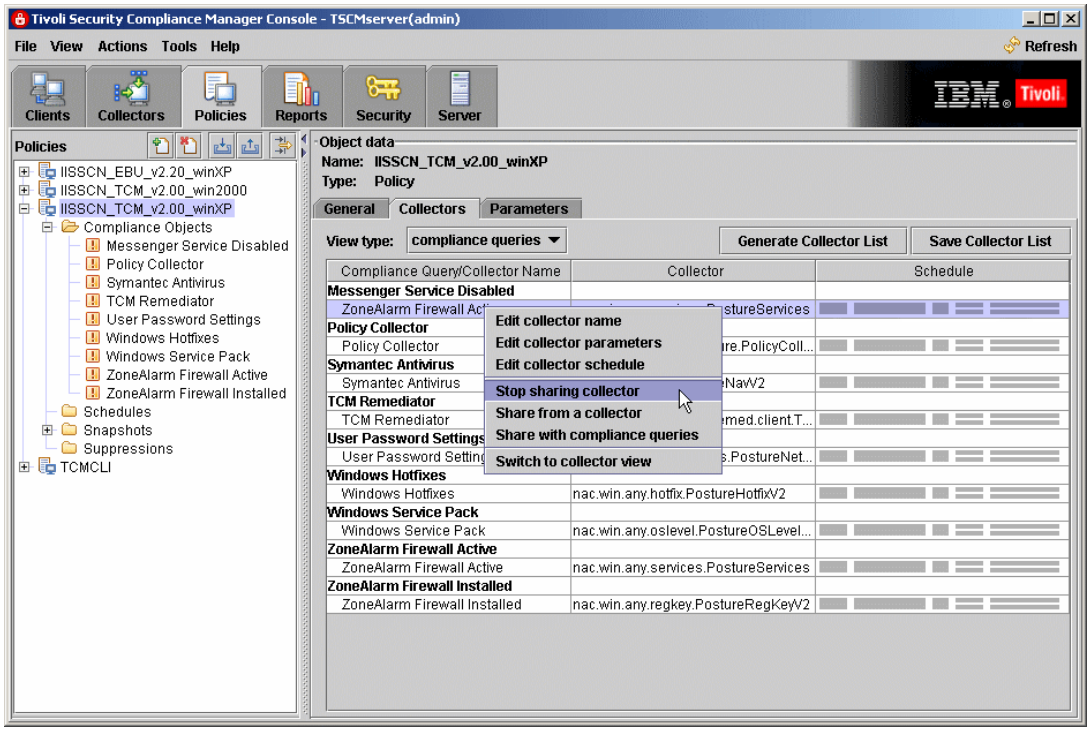


Figure 6-51 Disabling collector sharing

A small dialog window is displayed asking you for the new name of the collector instance. Enter `Messenger Service Disabled`, as shown in Figure 6-52, and click **OK**.

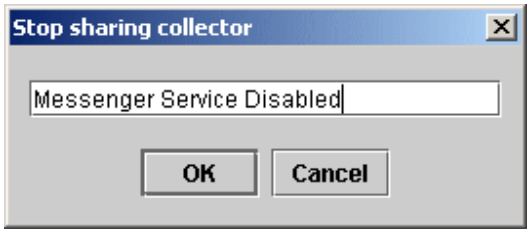


Figure 6-52 New collector instance name dialog

Downloaded from www.Manualslib.com manuals search engine

Now we must change the parameters for the new collector instance. Right-click the **Messenger Service Disabled** collector instance and click **Edit collector parameters** from the pop-up menu. The parameters were described in Table 6-7 on page 177. Provide the following parameter values:

- SERVICE_REQ equal to Messenger
- REQ_RUNNING not set
- SERVICE_RUNNING_WF not set
- REQ_DISABLED equal to 1
- SERVICE_DISABLED_WF equal to TCRMessengerDisabled

When you are done editing click **Save**.

3. As a final step save the changes you made to all of the collectors. If there are any changes that have not yet been saved the **Save Collector List** button on the right side of the window is active, as shown in Figure 6-53. Click this button.

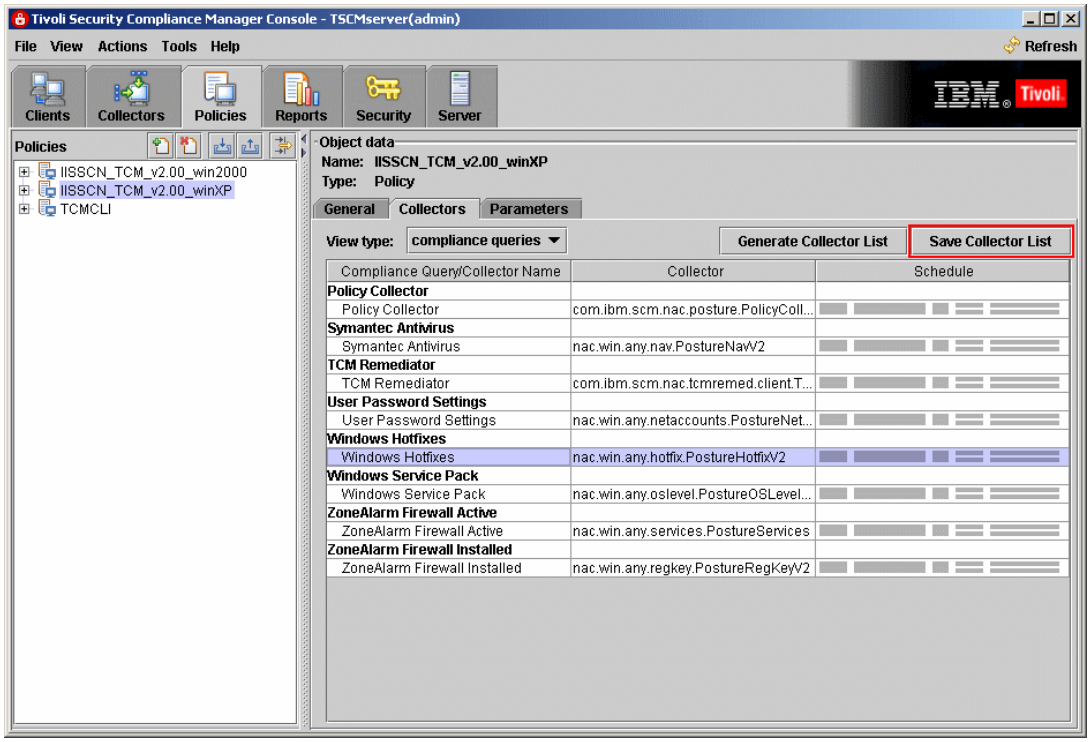


Figure 6-53 Saving changes made to the policy collectors

Downloaded from www.Manualslib.com manuals search engine

You are presented with a warning that the changes will affect all of the clients that have this policy assigned, as shown in Figure 6-54.

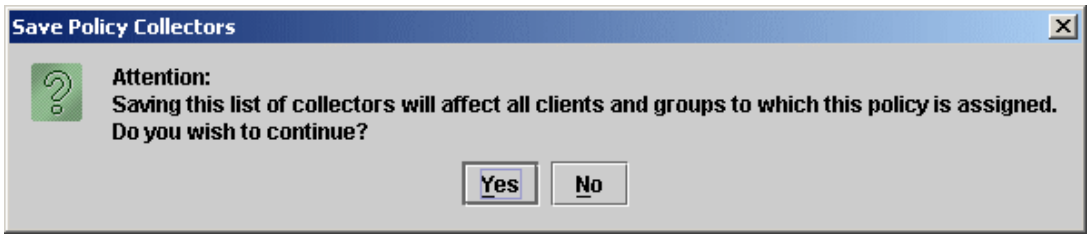

Save Policy Collectors
Attention:
Saving this list of collectors will affect all clients and groups to which this policy is assigned.
Do you wish to continue?
Yes
No

Figure 6-54 Save policy collectors warning

Click **Yes** to have your changes saved.

If you have different groups of clients in your environment with different operating systems or different requirements you may need to add more policies, repeating the steps described above for each policy and setting the correct values as appropriate.

6.2.5 Assigning the policy to the clients

To have the policy assigned to all client workstations in a consistent way we create a group for those clients and assign the policy to this group. Then when any new client is added to the group it will be automatically assigned with the latest policy version.

Downloaded from www.Manualslib.com manuals search engine

The steps are:

1. When logged into the Tivoli Security Compliance Manager Administration Console with administrative privileges select the **Clients** tab and click the **Actions** → **Group** → **Create Group** menu item, as shown in Figure 6-55.

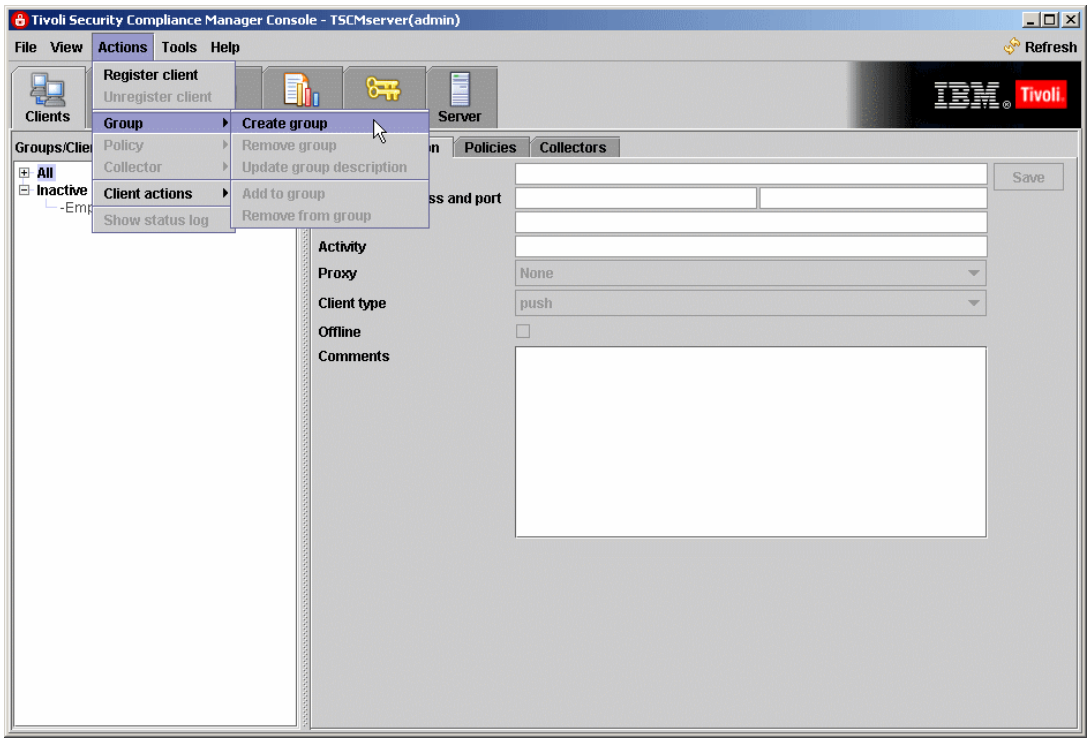


Figure 6-55 Create group action selection

2. On the Create group dialog, which is displayed in Figure 6-56, enter the name you want for your group (for example, NAC Windows XP) and click **OK**.

Figure 6-56 Create group dialog

Downloaded from www.Manualslib.com manuals search engine

3. Assign the policy to this new group. Select the group in the navigation tree in the left pane and click **Actions** →**Policy** → **Add policy**, as shown in Figure 6-57.

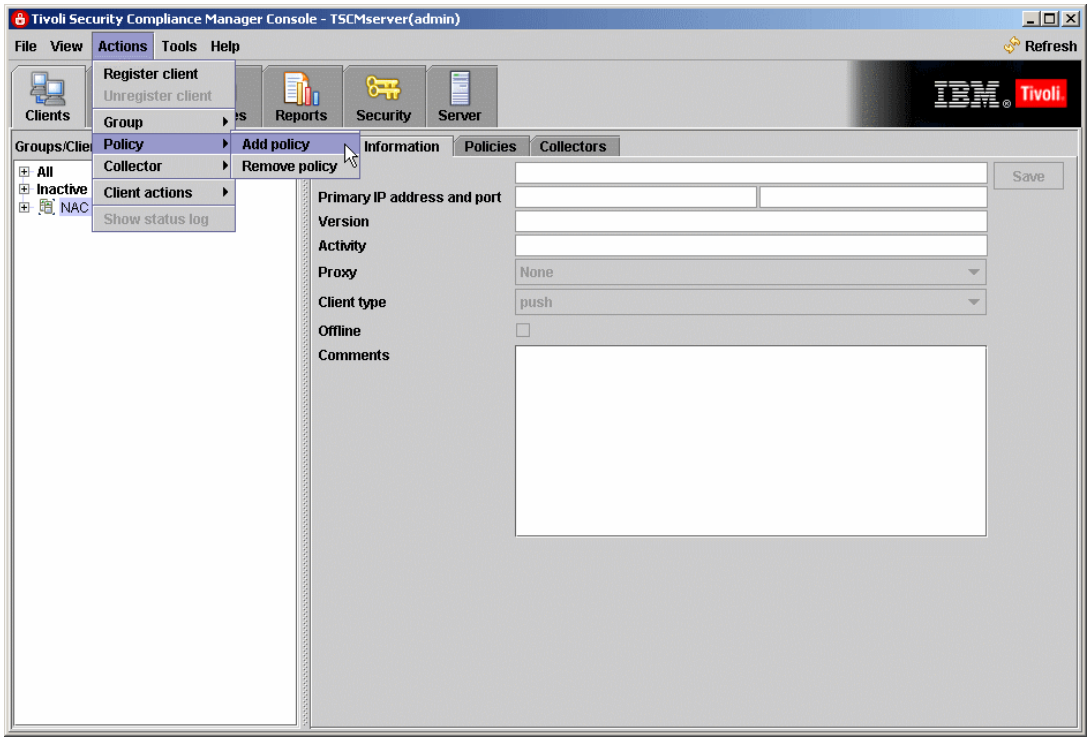


Figure 6-57 Add policy menu selection

4. The Select a policy window is displayed, as shown in Figure 6-58. Select the **IISSCN_TCM_v2.00_winXP** policy (the one we changed in 6.2, “Configuration of the compliance policies” on page 152) and click **OK**.

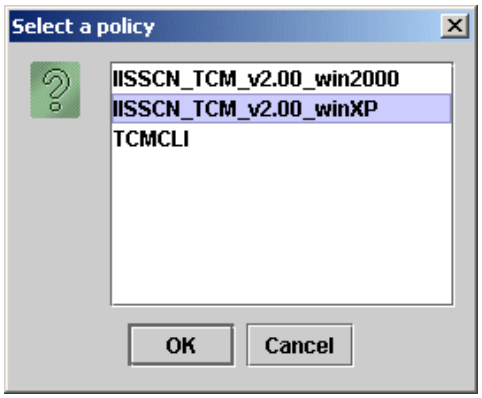


Figure 6-58 Policy selection window

Downloaded from www.Manualslib.com manuals search engine

5. An informational dialog is displayed, as shown in Figure 6-59, showing the successful completion. To close it click **OK**.

Figure 6-59 Operation complete dialog

6. Repeat steps 3 to 5 to select the TCMCLI policy this time. When you have your group selected in the left pane and you click the **Policies** tab in the right pane you should see a window similar to the one presented in Figure 6-60.

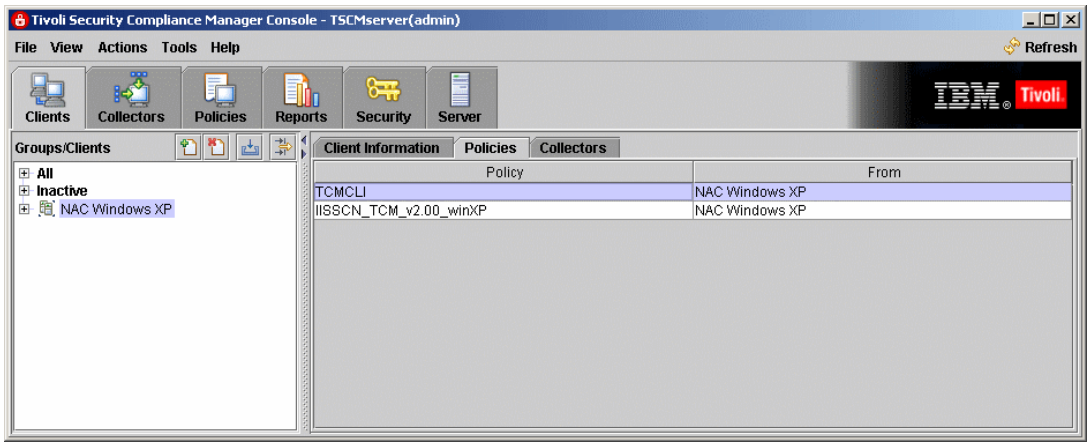


Figure 6-60 Policies assigned to the group

TCMCLI utility policy

The TCMCLI is the utility policy that associates the Tivoli Configuration Manager CLI back end for use by the Tivoli Security Compliance Manager remediator. The query in this policy is designed to never generate a violation, and this entry serves as a placeholder to import the TCMCLI collector into the policy.

This policy has to be assigned to every client workstation in order for the Tivoli Configuration Manager remediation workflows to work.

6.3 Deploying the client software

The second software element required for the NAC solution is the Security Compliance Manager client. The client is supported on many platforms. In this

Downloaded from www.Manualslib.com manuals search engine

book we cover only the installation of the client on Windows. For other platforms and more detailed system prerequisites see *Tivoli Security Compliance Manager: Installation Guide: Client Component*, GC32-1593. A prerequisite for the Security Compliance Manager client to work within the IBM Integrated Security Solution for Cisco Networks is the already deployed Cisco Trust Agent. This is why we first cover the installation of this component.

6.3.1 Cisco Trust Agent

The installation of the Cisco Trust Agent is an essential part of the client software deployment. It requires three steps to be performed, which in specific cases can be combined into two or even into one. These three steps are:

1. Installation of the Cisco Trust Agent base code
2. Installation of the ACS server certificate
3. Installation of one or more posture plug-ins

Prerequisites

Since the release of NAC phase 2, the Cisco Trust Agent version has been updated, and is available in two different options. There is the Cisco Trust Agent for Windows *with* a dot1x supplicant, and the Cisco Trust Agent for Windows *without* a dot1x supplicant. This section focuses on the Cisco Trust Agent *with* the dot1x supplicant. The installation packages of the Cisco Trust Agent can be downloaded from Cisco Connection Online (CCO) at:

`http://www.cisco.com`

You must have a valid CCO user ID and password to access this information. When we wrote this book the latest available version was 2.0.1.14. However, for this book we used Version 2.0.0.30. The installation package consists of a single executable file: ctasetup-supplicant-win-2.0.0.30.exe. Note that this file is for Windows XP only.

Note: You can use the CTA with the dot1x supplicant in an L2IP environment, in the case of future dot1x migration.

Refer to the CCO for the latest information about additional platform support.

Important: If your client is using personal firewall software, even if the service is disabled, it may block some communication. We recommend leaving the firewall software running but configuring it to grant Cisco Trust Agent communication on port 21862/udp if using L2/L3 IP NAC. *This is not necessary for NAC L2Dot1X.*

Downloaded from www.Manualslib.com manuals search engine

Note: The following section is an excerpt from the *Administrator Guide for Cisco Trust Agent 2.0*, which is available at (requires CCO login):

http://www.cisco.com/en/US/partner/products/ps5923/products_maintenance_guide_book09186a008059a40e.html

For Cisco Secure ACS to establish a secure PEAP session with Cisco Trust Agent, you must install the root certificate for the Cisco Secure ACS certificate on the network client. This certificate is either the CA certificate that is used to validate the server certificate, or a self-signed certificate generated by the Cisco Secure ACS server. Cisco Trust Agent supports PEM wrapped Base-64 or DER encoded binary X.509 certificates.

The installation of the certificate that is required for secure communication with the Cisco Secure ACS can be performed during the installation of the Cisco Trust Agent or later using the ctaCert.exe utility.

To have the certificate installed during the Cisco Trust Agent setup, create a Certs directory in the directory where the setup executable is located and put the certificate file into this directory (Figure 6-61). The certificate is picked up automatically by the setup process.

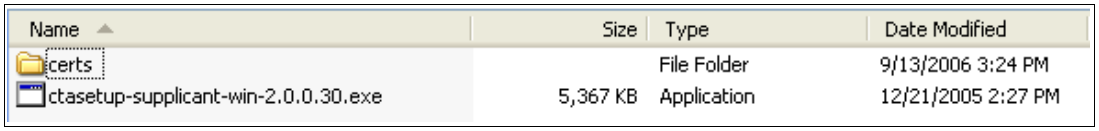


Figure 6-61 Certs directory with CTA

Which certificate to use depends on the Cisco Secure ACS infrastructure in the network. If the Cisco Secure ACS is using Certificate Authority (CA) signed certificates, you have to use the root CA certificate. If the Cisco Secure ACS is using a self-signed certificate, you have to extract and use this certificate.

Important: If there is more than one Cisco Secure ACS in the environment, all of the respective certificates should be installed along with the Cisco Trust Agent.

The procedure of extracting the Cisco Secure ACS certificate is described in 7.1.1, “Configuring the Cisco Secure ACS for NAC L2 802.1x” on page 214.

Downloaded from www.Manualslib.com manuals search engine

Installation of Cisco Trust Agent on Windows

The Cisco Trust Agent installation uses the Microsoft Windows Installer (MSI) and requires administrator privileges.

1. Start the installation process by double-clicking the setup file or typing the command:

   ```
   ctasetup-supplicant-win-2.0.0.30.exe
   ```

2. After starting the setup file, the welcome window opens (Figure 6-62). Click **Next**.

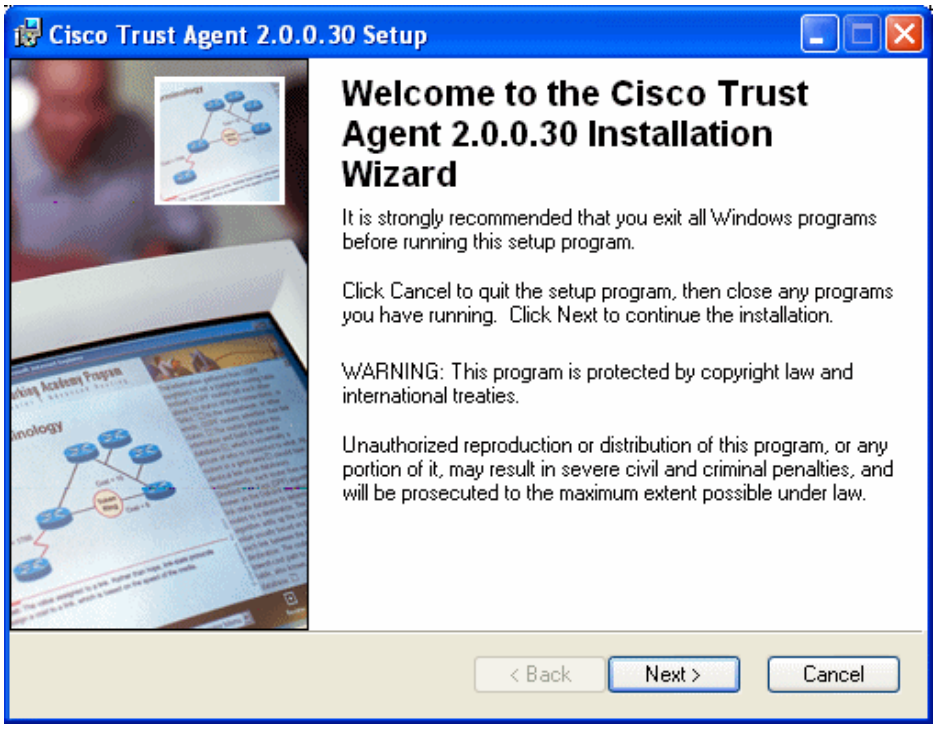

Cisco Trust Agent 2.0.0.30 Setup
Welcome to the Cisco Trust Agent 2.0.0.30 Installation Wizard
It is strongly recommended that you exit all Windows programs before running this setup program.
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
< Back
Next >
Cancel

Figure 6-62 Cisco Trust Agent installation wizard

Downloaded from www.Manualslib.com manuals search engine

3. The license agreement is presented, as shown in Figure 6-63. Select **I accept the license agreement** and click **Next**.

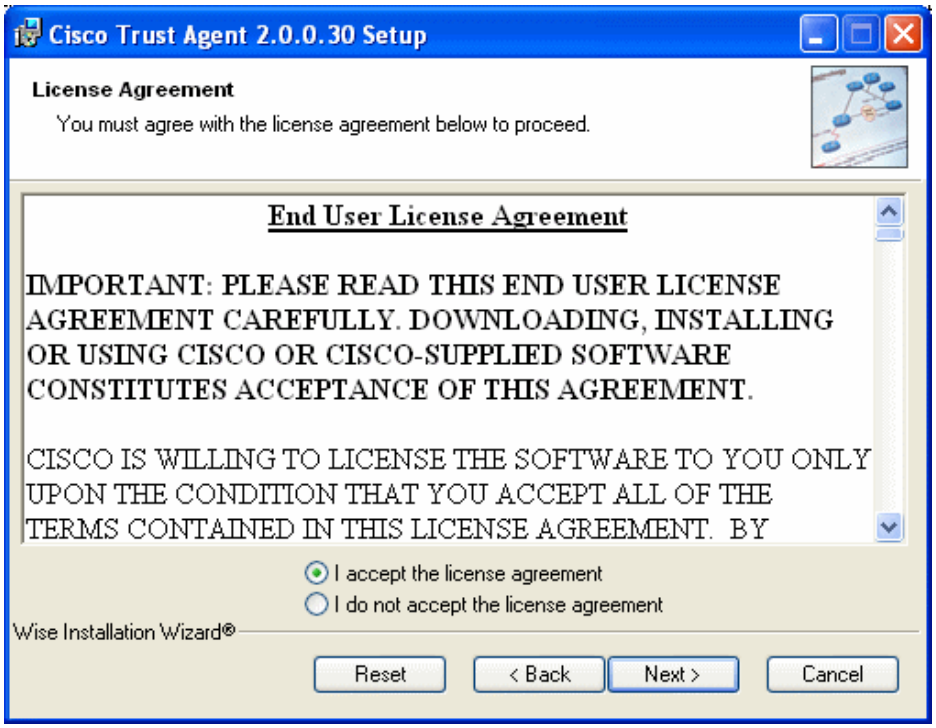

Cisco Trust Agent 2.0.0.30 Setup
License Agreement
You must agree with the license agreement below to proceed.
End User License Agreement
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY
I accept the license agreement
I do not accept the license agreement
Wise Installation Wizard®
Reset
< Back
Next >
Cancel

Figure 6-63 License agreement for Cisco Trust Agent

Downloaded from www.Manualslib.com manuals search engine

4. Accept the defaults (Figure 6-64) and click **Next**.

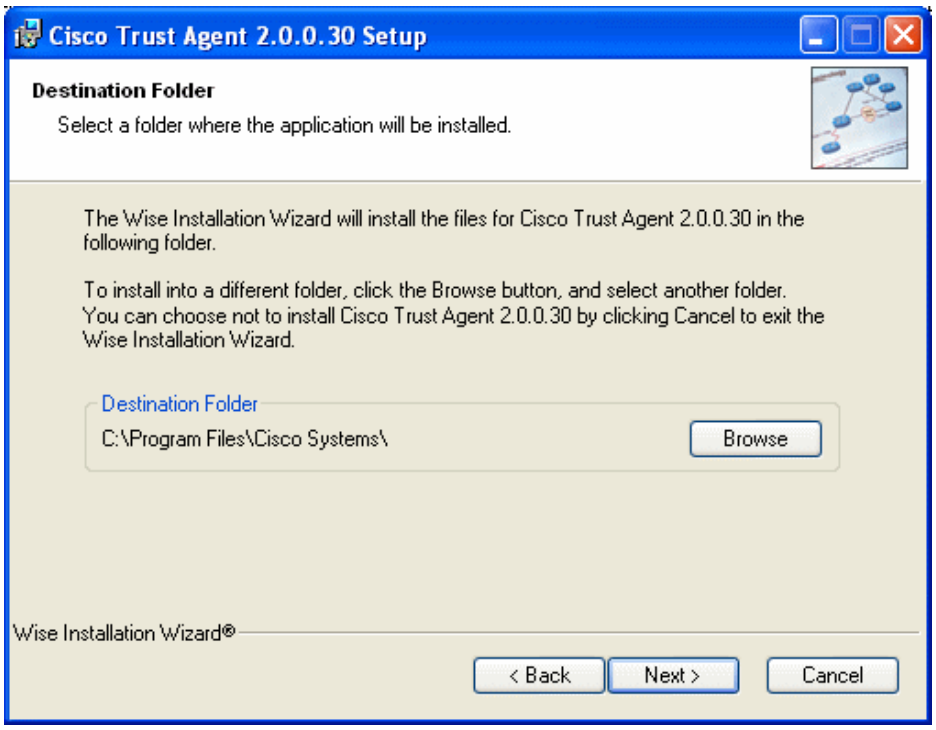

Cisco Trust Agent 2.0.0.30 Setup
Destination Folder
Select a folder where the application will be installed.
The Wise Installation Wizard will install the files for Cisco Trust Agent 2.0.0.30 in the following folder.
To install into a different folder, click the Browse button, and select another folder.
You can choose not to install Cisco Trust Agent 2.0.0.30 by clicking Cancel to exit the Wise Installation Wizard.
Destination Folder
C:\Program Files\Cisco Systems\
Browse
Wise Installation Wizard®
< Back
Next >
Cancel

Figure 6-64 Cisco Trust Agent destination folder selection

Downloaded from www.Manualslib.com manuals search engine

5. Accept the default depicted in Figure 6-65 and click **Next**.

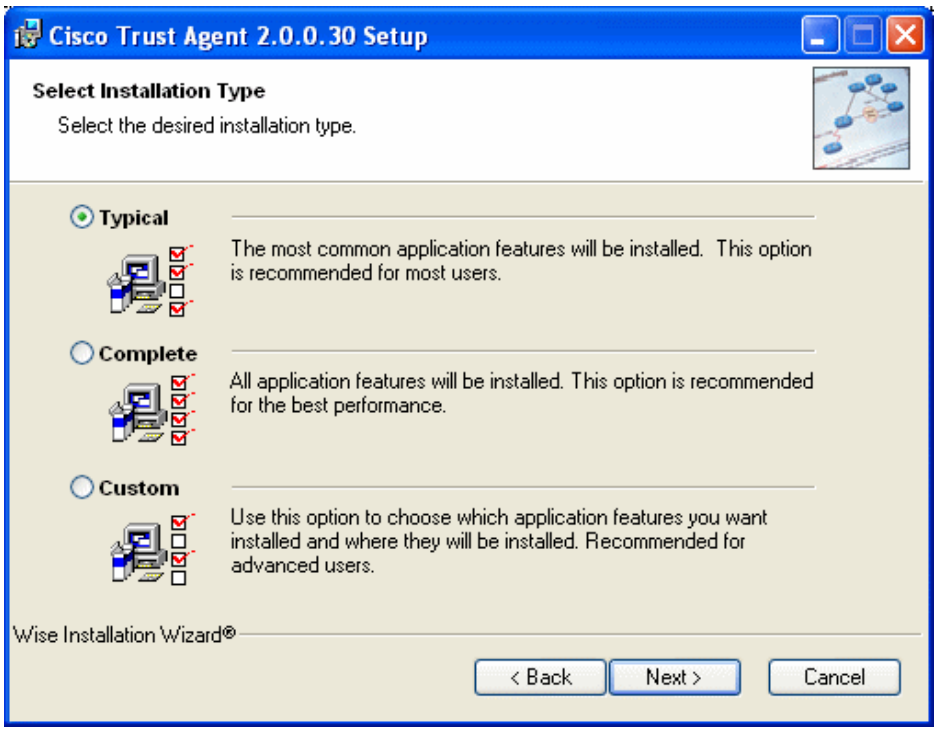

Cisco Trust Agent 2.0.0.30 Setup
Select Installation Type
Select the desired installation type.
Typical
The most common application features will be installed. This option is recommended for most users.
Complete
All application features will be installed. This option is recommended for the best performance.
Custom
Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.
Wise Installation Wizard®
< Back
Next >
Cancel

Figure 6-65 Cisco Trust Agent installation type

Downloaded from www.Manualslib.com manuals search engine

6. Click **Next** (Figure 6-66).

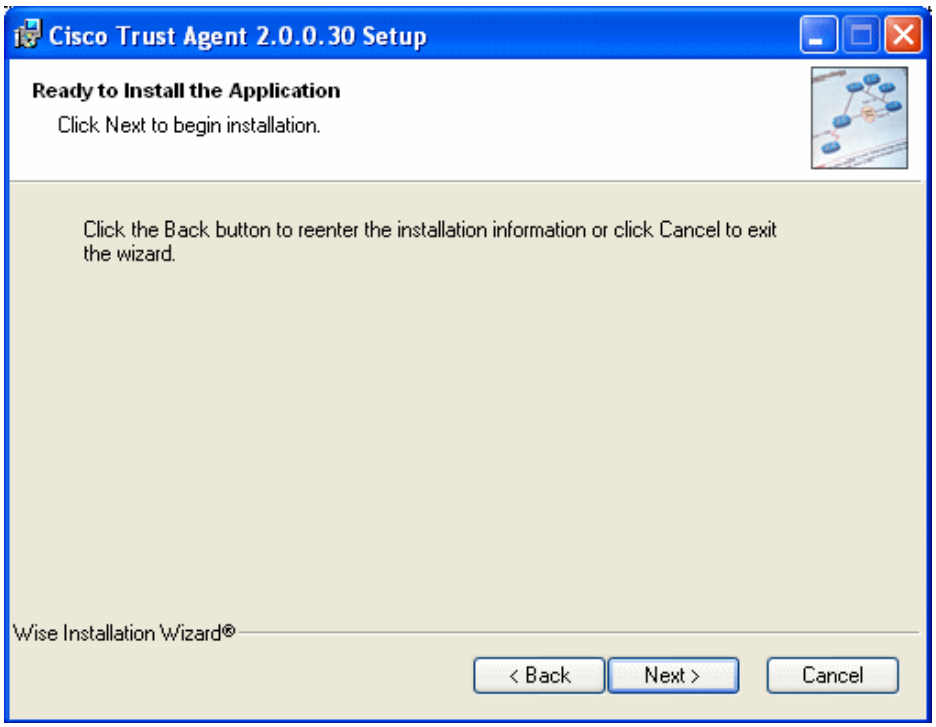

Cisco Trust Agent 2.0.0.30 Setup
Ready to Install the Application
Click Next to begin installation.
Click the Back button to reenter the installation information or click Cancel to exit the wizard.
Wise Installation Wizard®
< Back
Next >
Cancel

Figure 6-66 Ready to install the Cisco Trust Agent application

Downloaded from www.Manualslib.com manuals search engine

7. If the certificate file was copied into the Certs directory, the window in Figure 6-67 is presented during the installation. Click **OK**. Remember, this step is optional and will only be presented if you have copied the certificate file to the Certs directory.

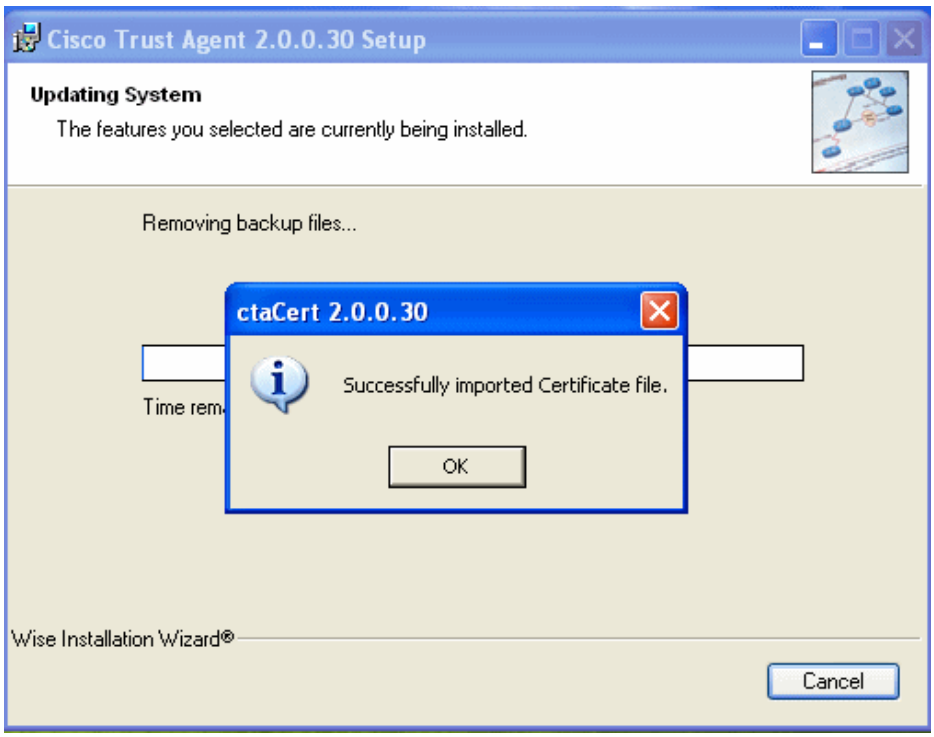


Figure 6-67 Confirmation of the certificate import

Downloaded from www.Manualslib.com manuals search engine

8. Click **Finish** to close the installation, as shown in Figure 6-68.

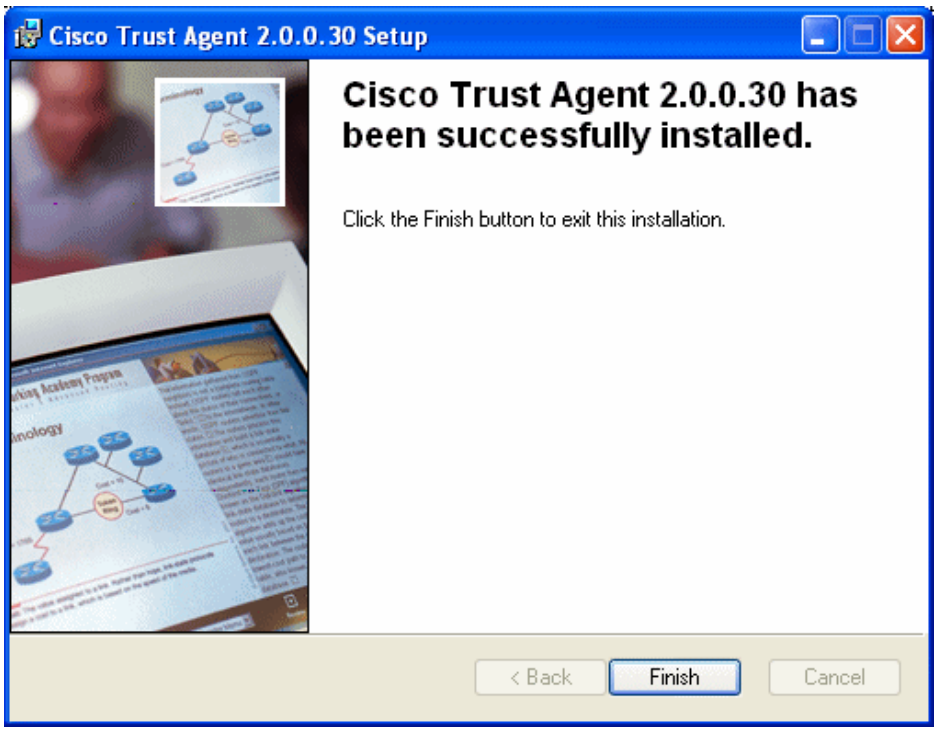

Cisco Trust Agent 2.0.0.30 Setup
Cisco Trust Agent 2.0.0.30 has been successfully installed.
Click the Finish button to exit this installation.
< Back
Finish
Cancel

Figure 6-68 Successful completion of Cisco Trust Agent installation

9. If you have not created a Certs directory before the installation as described in “Prerequisites” on page 190 or you were not presented with the window shown in Figure 6-67 on page 197 during the installation, install the certificates manually using the ctaCert.exe utility. This utility is located in the CiscoTrustAgent subdirectory of the installation directory you selected in step 5 on page 195. The syntax for the command is shown below:

```
ctaCert.exe /add "<path to the certificate file>" /store "Root"
```

For more information about the utility refer to the *Administrator Guide for Cisco Trust Agent 2.0*, which is available at (requires CCO login):

http://www.cisco.com/en/US/partner/products/ps5923/products_maintenance_guide_book09186a008059a40e.html

Downloaded from www.Manualslib.com manuals search engine

If the certificate has been successfully imported, the window shown in Figure 6-69 is displayed.

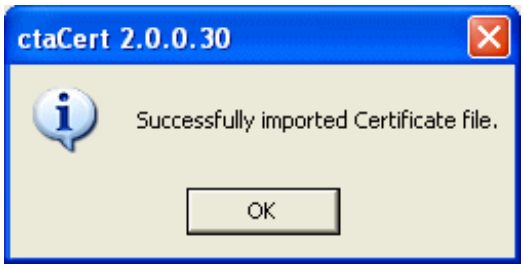


Figure 6-69 Successful certificate import

Tip: The ctaCert.exe utility seems to have a problem with long path names. If you have received an error message, ensure that the path to the certificate file is correct, and if the path (including the file name) is very long, move the file to a different location and try again.

The last element required by the Cisco Trust Agent to perform its role is the posture plug-in. In our scenario this element is installed automatically during the Security Compliance Manager client setup.

6.3.2 IBM Tivoli Security Compliance Manager client

In this section we describe the installation of Tivoli Security Compliance Manager client. It is a requirement to have the Cisco Trust Agent already installed before starting the Tivoli Security Compliance Manager client installation.

Downloaded from www.Manualslib.com manuals search engine

The Security Compliance Manager client installation requires the following media: Security Compliance Manager 5.1.0.30 client base installation image.

Installation of the Security Compliance Manager client

The procedure of the client installation is very similar to the server installation. Both are using the same type of Java installer, however, since this version of the client is running a different version of JVM™ and the installation files were separated. To perform the installation follow the steps described below.

1. Start the installation by running the setup file named scmclient_win32.exe from the Security Compliance Manager 5.1 FP30 installation CD. After a few seconds, which are required to start the Java virtual machine, the language selection box opens (Figure 6-70). Select your preferred language for the installation wizard and click **OK**.

Figure 6-70 Language selection

Downloaded from www.Manualslib.com manuals search engine

2. The Security Compliance Manager welcome screen appears momentarily (Figure 6-71).

IBM
Tivoli.
Security Compliance Manager
Version 5.1.0
Copyright © 2003, 2004 By IBM Corporation. All Rights Reserved. Java based marks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, or both. See product license for details.
Java
COMPATIBLE

Figure 6-71 The welcome window

Downloaded from www.Manualslib.com manuals search engine

3. The Client Installation Utility window appears, as depicted in Figure 6-72. After carefully reading all of the required information, click **Next**.

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
IBM Tivoli Security Compliance Manager
Version 5.1.0.30
Client Installation Utility
You are about to install a Client component of IBM Tivoli Security Compliance Manager, Version 5.1.0.30.
Required Information
Descriptions of the components and the information you will need to supply during their installation are listed below. For more information, please see the IBM Tivoli Security Compliance Manager Installation Guide.
InstallShield
< Back
Next >
Cancel

Figure 6-72 Client Installation Utility window

Downloaded from www.Manualslib.com manuals search engine

4. The license agreement window is displayed (Figure 6-73). Select **I accept the terms in the license agreement** and click **Next**.

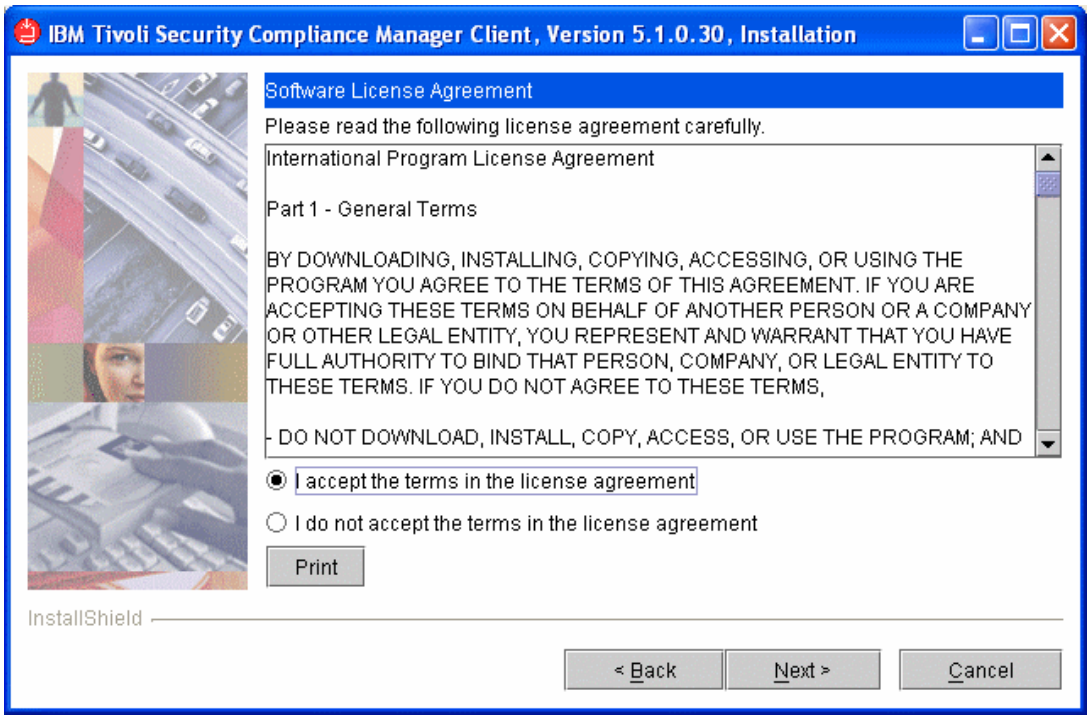

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

Figure 6-73 License agreement for IBM Tivoli Security Compliance Manager

Downloaded from www.Manualslib.com manuals search engine

5. Accept the default destination folder, shown in Figure 6-74, and click **Next**.

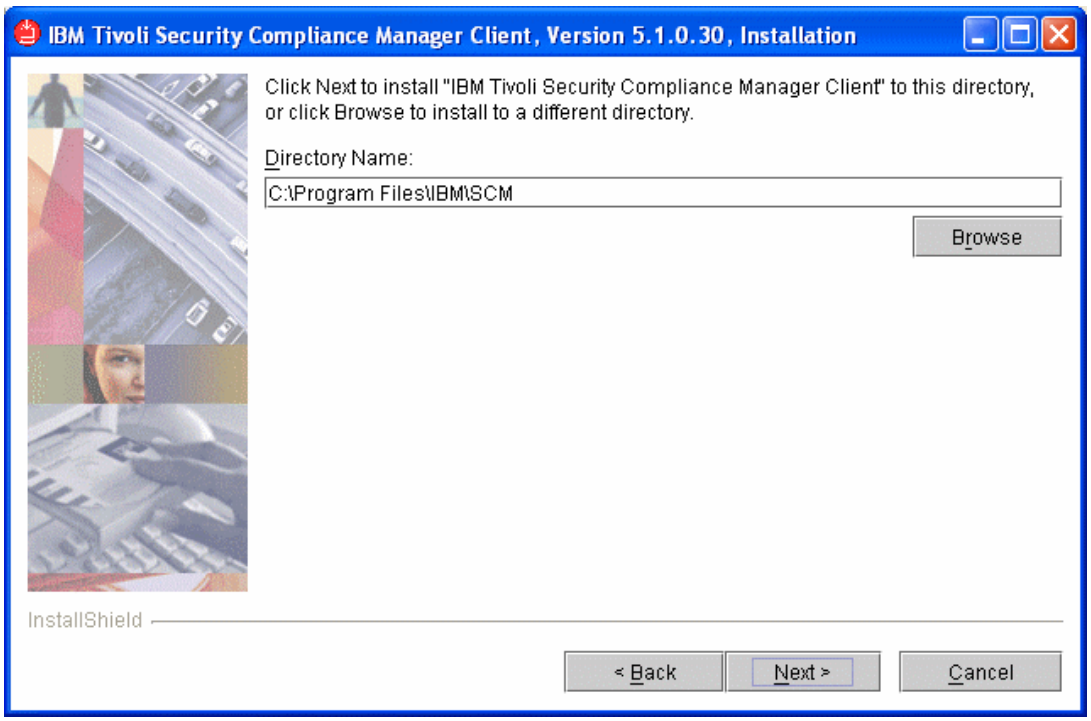

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Click Next to install "IBM Tivoli Security Compliance Manager Client" to this directory, or click Browse to install to a different directory.
Directory Name:
C:\Program Files\IBM\SCM
Browse
InstallShield
< Back
Next >
Cancel

Figure 6-74 Directory selection window

Downloaded from www.Manualslib.com manuals search engine

6. Accept the default client installation (Figure 6-75) and click **Next**.

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Choose the setup type that best suits your needs.
IBM Tivoli Security Compliance Manager Client
The IBM Tivoli Security Compliance Manager Client runs collectors that are used by the IBM Tivoli Security Compliance Manager Server to monitor compliance with security policies.
InstallShield
< Back
Next >
Cancel

Figure 6-75 Setup type window

Downloaded from www.Manualslib.com manuals search engine

7. In the IBM Security Solution for Cisco Networks window (Figure 6-76), ensure that the box **Select the checkbox to install IBM Integrated Security Solution for Cisco Networks** is checked, then click **Next**

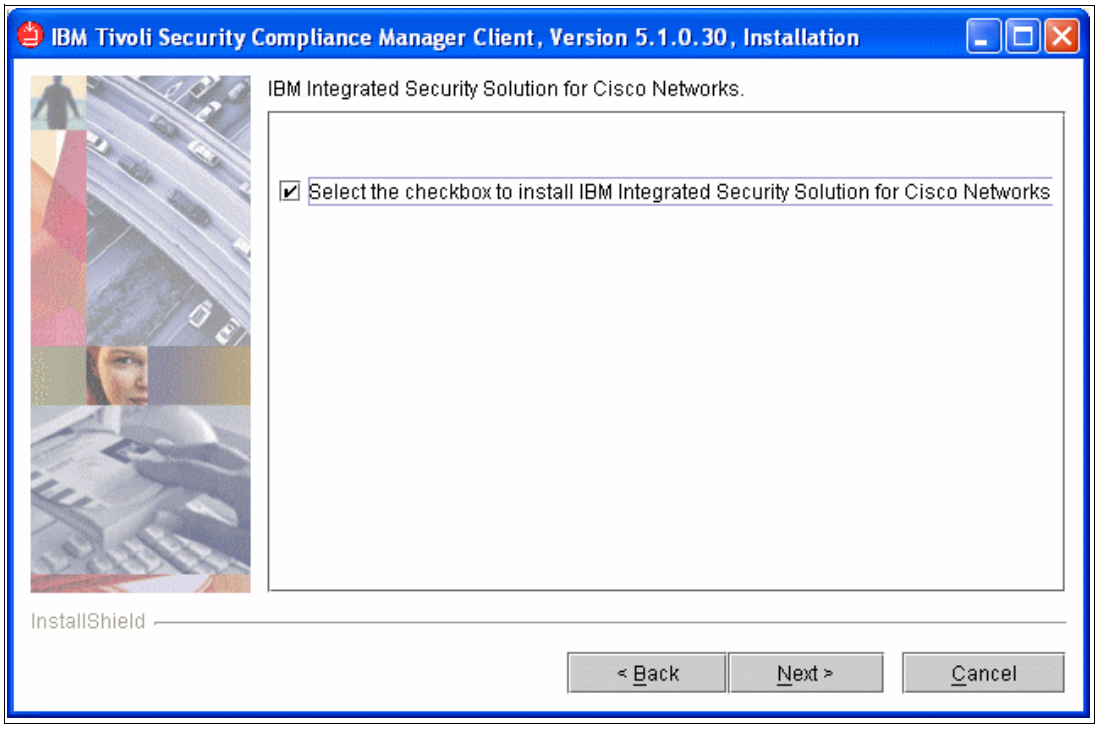

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
IBM Integrated Security Solution for Cisco Networks.
Select the checkbox to install IBM Integrated Security Solution for Cisco Networks
InstallShield
< Back
Next >
Cancel

Figure 6-76 The IBM Integrated Security Solution for Cisco Networks window

8. In the client communication mode window, select the port on which the client listens for requests. The default port is 1950.

   The client can operate in one of these communication modes:

   Push This is the mode in which communication can be initiated from both sides, client and server. This is the recommended mode for workstations, as only this mode enables the client to use DHCP administered IP addresses.

   Pull In this mode the client listens for server requests, but the server always initiates communication sessions. This setting is useful for traffic across a firewall, but only for static IP addresses.

   Note: Push mode is the more scalable approach. Use pull mode only when absolutely required.

   Accept the defaults and click **Next**.

Downloaded from www.Manualslib.com manuals search engine

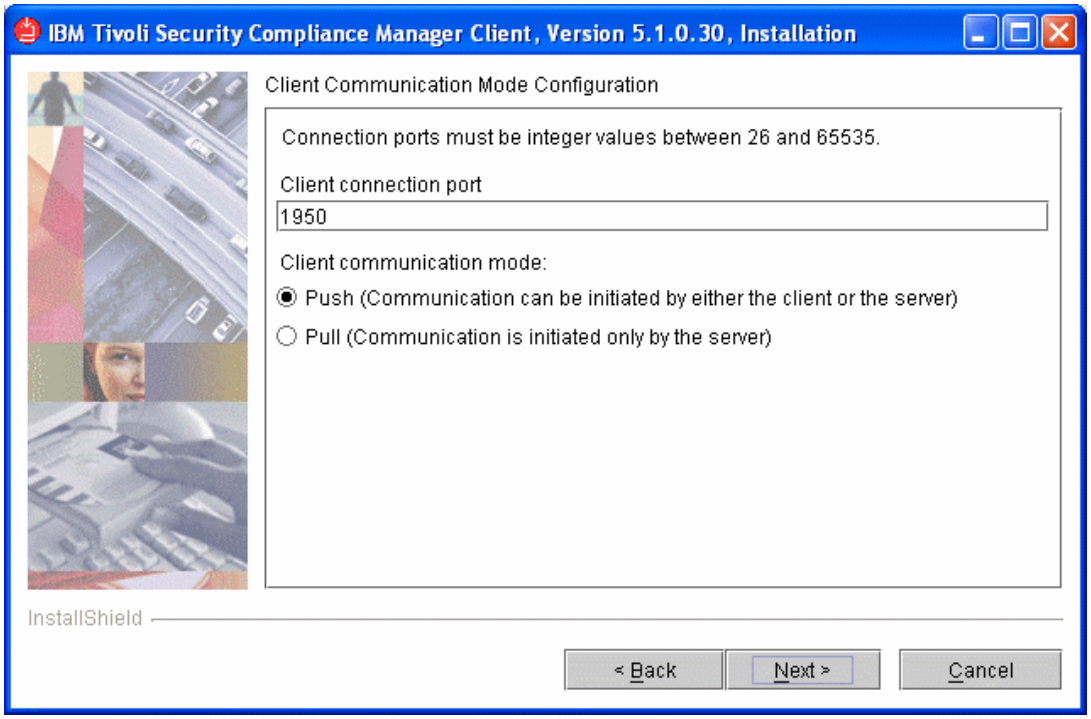

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Client Communication Mode Configuration
Connection ports must be integer values between 26 and 65535.
Client connection port
1950
Client communication mode:
Push (Communication can be initiated by either the client or the server)
Pull (Communication is initiated only by the server)
InstallShield
< Back
Next >
Cancel

Figure 6-77 Client connection window

Downloaded from www.Manualslib.com manuals search engine

9. The server communication configuration window, shown in Figure 6-78, is used to provide the client with the location information of the server. In the Server host name field insert the fully qualified name of the Security Compliance Manager server (or IP address). The default value for the Server connection port field is 1951. Unless you have selected a different port number during the server installation, accept the default.

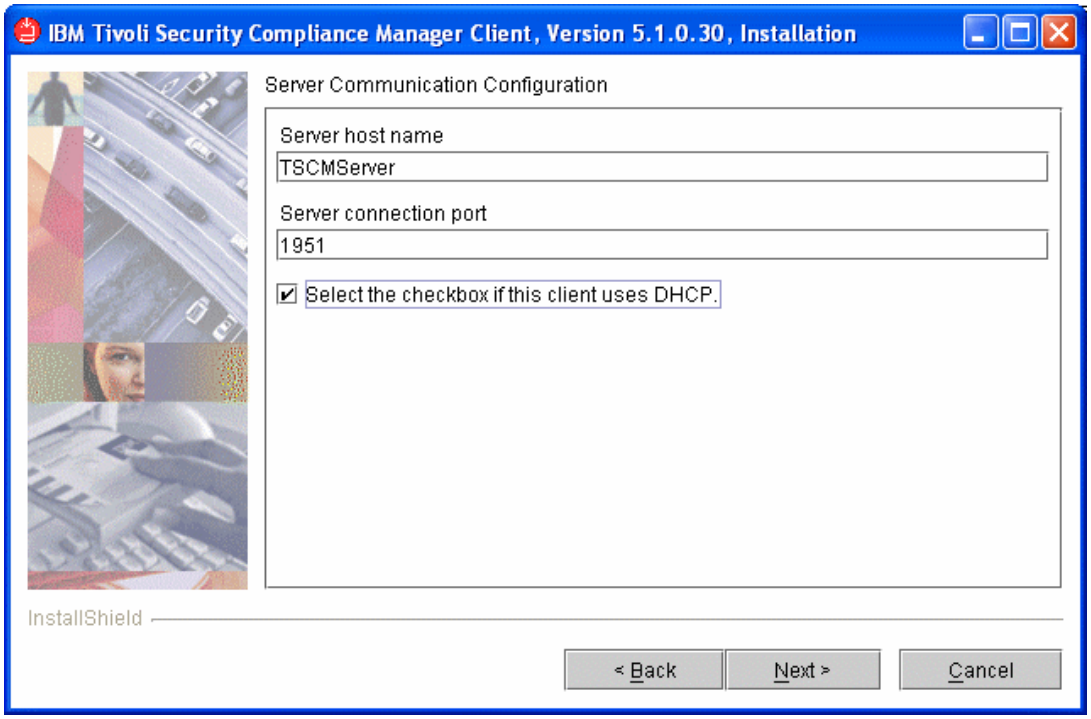


Figure 6-78 Server communication configuration window

Tip: When using a fully qualified domain name, it is always a good idea to check the DNS names resolution by opening a command prompt window and trying to **`ping`** the server by name.

If you selected the push mode in the previous step, you will be given an option to indicate whether the client uses DHCP. *This is mandatory for clients using DHCP* but we recommend checking this option even on clients using a static IP address, as this results in the generation of a 16-byte unique identifier (fingerprint) for the client.

When you are done, click **Next**.

Downloaded from www.Manualslib.com manuals search engine

10. If you selected the DHCP option in the previous step, you will see the client DHCP configuration dialogue, as in Figure 6-79. In the DHCP client alias field, provide the alias name for the client. This name will be shown on the Security Compliance Manager server during client registration, and the client will be referenced by this name in the Security Compliance Manager GUI. If this field is left blank, the name that will appear in the Security Compliance Manager GUI will be the client's computer name.

    Enter the name you want (if any) and click **Next**.

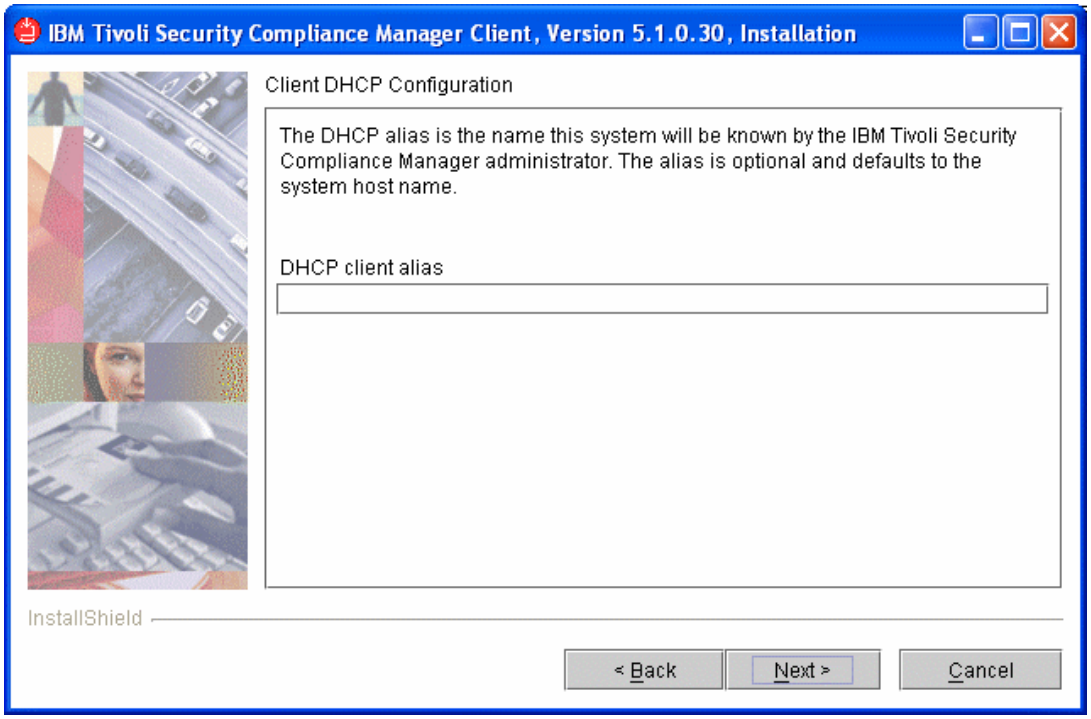

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Client DHCP Configuration
The DHCP alias is the name this system will be known by the IBM Tivoli Security Compliance Manager administrator. The alias is optional and defaults to the system host name.
DHCP client alias
InstallShield
< Back
Next >
Cancel

Figure 6-79 Client DHCP configuration window

Downloaded from www.Manualslib.com manuals search engine

11. Finally, the installation summary window is displayed (Figure 6-80). Click **Next**.

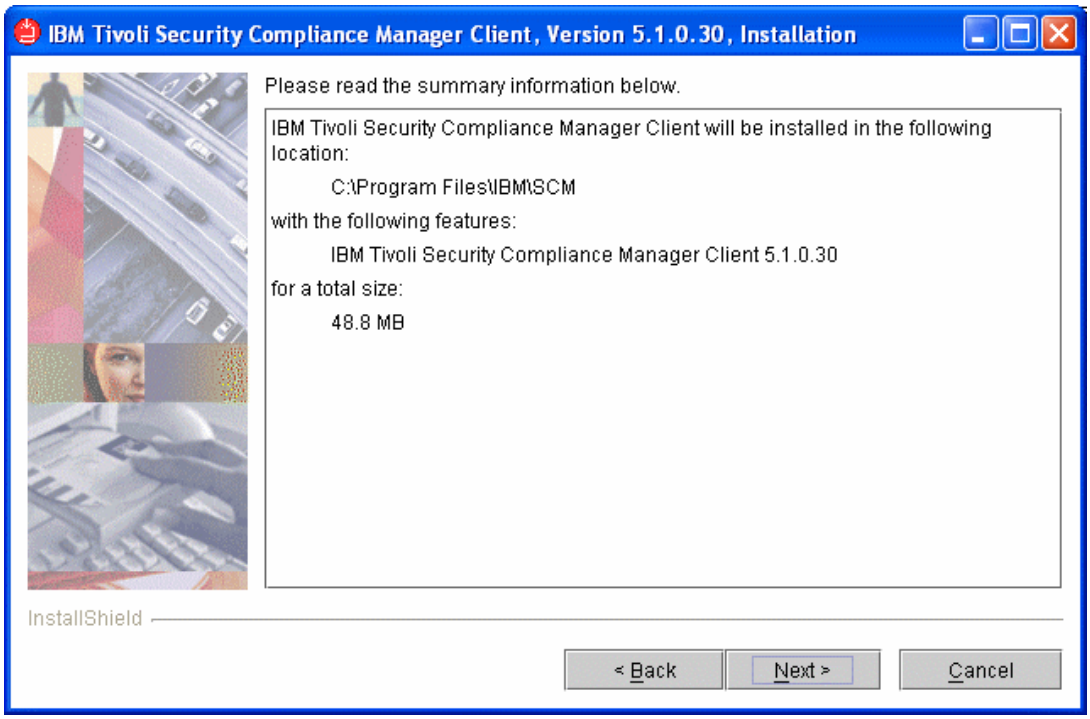

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Please read the summary information below.
IBM Tivoli Security Compliance Manager Client will be installed in the following location:
C:\Program Files\IBM\SCM
with the following features:
IBM Tivoli Security Compliance Manager Client 5.1.0.30
for a total size:
48.8 MB
InstallShield
< Back
Next >
Cancel

Figure 6-80 Security Compliance Manager client installation summary window

Downloaded from www.Manualslib.com manuals search engine

12. The Security Compliance Manager client is successfully installed. Click **Finish** to close the window shown in Figure 6-81 to complete this step of the process.

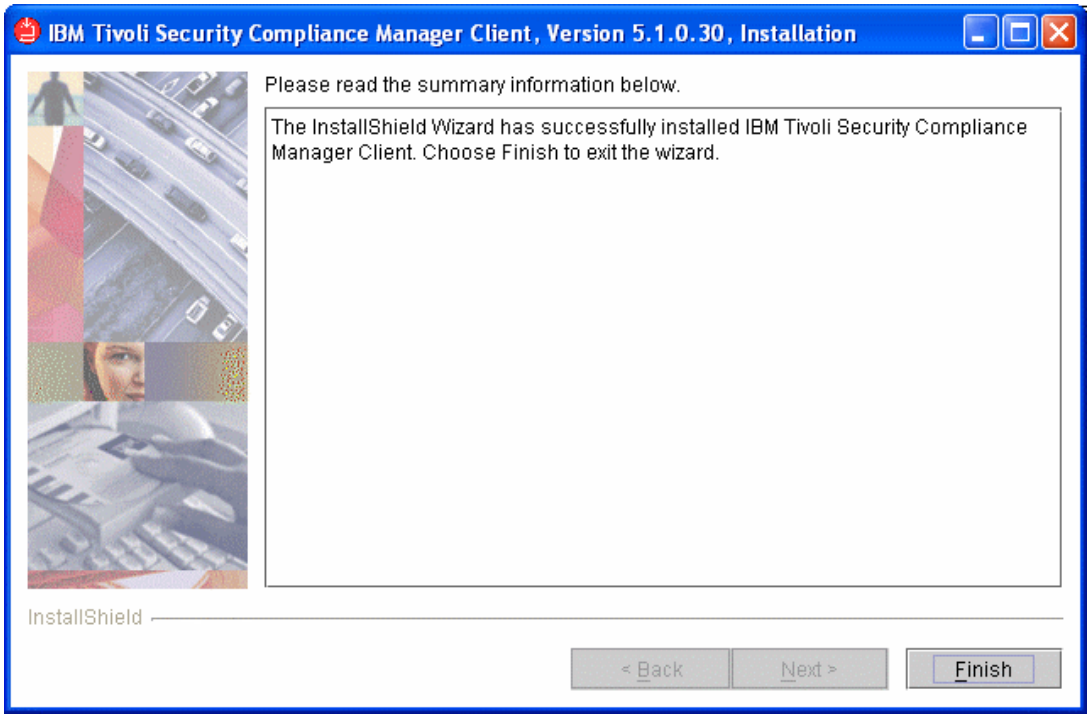

IBM Tivoli Security Compliance Manager Client, Version 5.1.0.30, Installation
Please read the summary information below.
The InstallShield Wizard has successfully installed IBM Tivoli Security Compliance Manager Client. Choose Finish to exit the wizard.
InstallShield
< Back
Next >
Finish

Figure 6-81 Successful completion window

Downloaded from www.Manualslib.com manuals search engine

13. If you want to verify that the Security Compliance Manager posture plug-in was registered successfully with the Cisco Trust Agent, check the C:\Program Files\Common Files\PostureAgent\Plugins directory. The ibmnac6.dll and ibmnac6.inf files should be there (Figure 6-82).

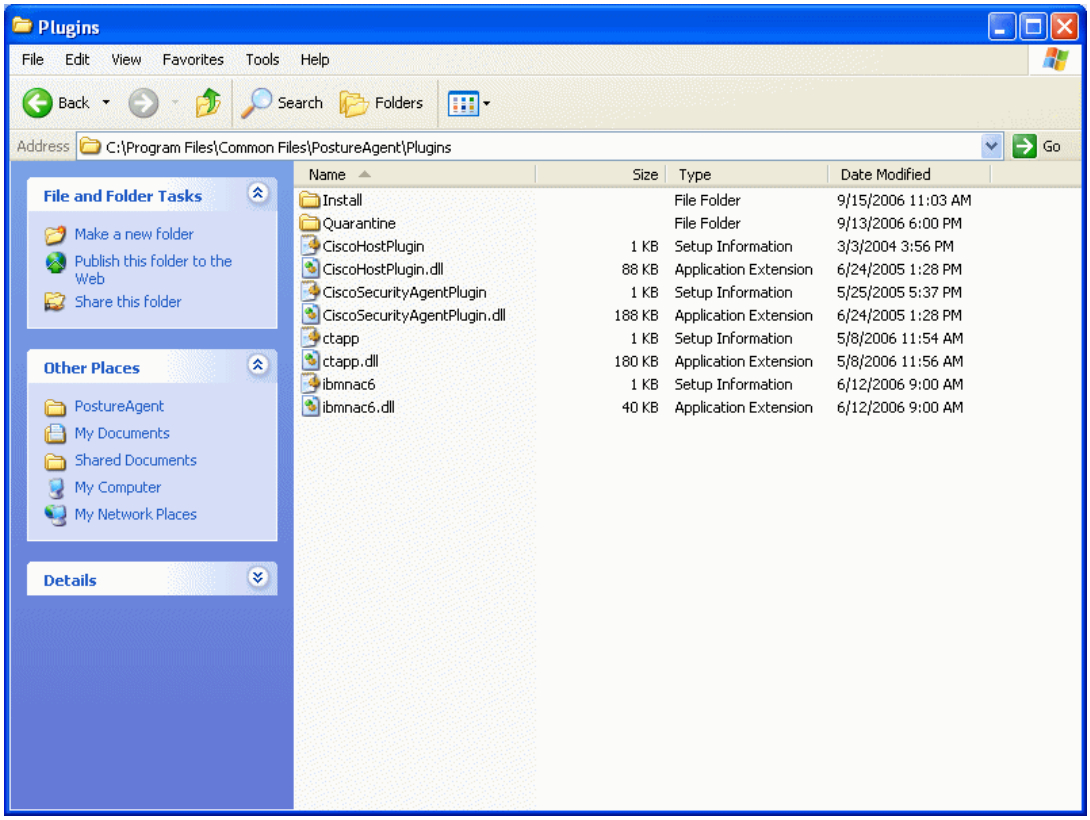

Plugins
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\Common Files\PostureAgent\Plugins
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
PostureAgent
My Documents
Shared Documents
My Computer
My Network Places
Details
Name Size Type Date Modified
Install File Folder 9/15/2006 11:03 AM
Quarantine File Folder 9/13/2006 6:00 PM
CiscoHostPlugin 1 KB Setup Information 3/3/2004 3:56 PM
CiscoHostPlugin.dll 88 KB Application Extension 6/24/2005 1:28 PM
CiscoSecurityAgentPlugin 1 KB Setup Information 5/25/2005 5:37 PM
CiscoSecurityAgentPlugin.dll 188 KB Application Extension 6/24/2005 1:28 PM
ctapp 1 KB Setup Information 5/8/2006 11:54 AM
ctapp.dll 180 KB Application Extension 5/8/2006 11:56 AM
ibmnac6 1 KB Setup Information 6/12/2006 9:00 AM
ibmnac6.dll 40 KB Application Extension 6/12/2006 9:00 AM

Figure 6-82 Security Compliance Manager posture plug-in files

6.4 Conclusion

This concludes the installation and configuration of the basic compliance subsystem. At this point you have established and assigned the security policy to the clients. We are also providing the following information for the other teams:

- The networking team must know the *policy name* to set up the policy on the Cisco ACS server.
- The remediation team must know the *names of the workflows* configured in the policy.

In the next chapters we describe the processes for these two teams.

Downloaded from www.Manualslib.com manuals search engine

7

Network enforcement subsystem implementation

This chapter contains detailed descriptions for the installation and configuration of the following network enforcement subsystem components:

- Configuring NAC Framework components
  - Configuring the Cisco Secure ACS for NAC L2 802.1x
  - Configuring the Cisco Secure ACS for NAC L2/L3 IP
  - Deployment of the network infrastructure
- Configuring NAC Appliance components
  - Installing the CCA Agent
  - Configuring Out-Of-Band Virtual Gateway Server
  - Deployment of the network infrastructure

Note: Although the installation for the Cisco Trust Agent client software logically belongs to the network enforcement subsystem implementation, it had to be installed prior to the Tivoli Security Compliance Manager client software covered in Chapter 6, “Compliance subsystem implementation” on page 125. The detailed instructions for setting up the CTA client can be found in 6.3.1, “Cisco Trust Agent” on page 190.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

7.1 Configuring NAC Framework components

This section focuses on the deployment of NAC Framework. NAC Framework can be deployed as NAC L3 IP, NAC L2 IP, or NAC L2 802.1x.

- Configure the Cisco Secure ACS for NAC L2 802.1x.
- Configure the Cisco Secure ACS for L2/L3 IP NAC.
- Deploy the network infrastructure (authenticator).
- Configure a Cisco 3750 switch with Cisco IOS software as a Network Access Device.

7.1.1 Configuring the Cisco Secure ACS for NAC L2 802.1x

Cisco Secure ACS is required to perform the NAC authentication server role and checking whether or not clients contain any violations to the deployed security policy.

The following steps detail the installation (where required) and configuration of the individual components that comprise the NAC feature:

1. Installing Cisco Secure ACS
2. Configuring the administrative interface to Cisco Secure ACS
3. Allowing administrator access via HTTP (optional)
4. Cisco Secure ACS certificate setup
5. Using an ACS self-signed certificate
6. Importing IBM Security Compliance Manager attributes
7. Configuring logging
8. Configuring a network device group in Cisco Secure ACS
9. Configuring RADIUS attributes
10. Configuring groups
11. Configuring users
12. Global authentication setup
13. Configuring posture validation
14. Configuring RADIUS Authorization Components
15. Configuring Network Access Profiles
16. Configuring external user databases
17. Unknown user policy
18. Clientless user

The *User Guide for Cisco Secure ACS for Windows 4.0* documentation can be found at (requires CCO login):

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_user_guide_book09186a0080533dd8.html

Downloaded from www.Manualslib.com manuals search engine

Installing Cisco Secure ACS

To install Cisco Secure ACS Version 4.0 software on a machine running a supported operating system, run the setup.exe program provided with the Cisco Secure ACS installation software. When you install Cisco Secure ACS, the setup program uninstalls any previous version of Cisco Secure ACS before it installs the new version. If you have a previous version, you are given the option to save and reuse your existing configuration.

For details about the install process refer to the *Installation Guide for Cisco Secure ACS for Windows 4.0,* located at:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_guide_book09186a0080533d5e.html

Use a Web interface to configure Cisco Secure ACS. After the initial configuration, point a Web browser to the IP address of the Cisco Secure ACS, using port 2002, for example, http://a.b.c.d:2002. The Welcome window opens (Figure 7-1). Log in and the main menu will be displayed. Use the buttons on the left frame of this window to select a specific configuration task.

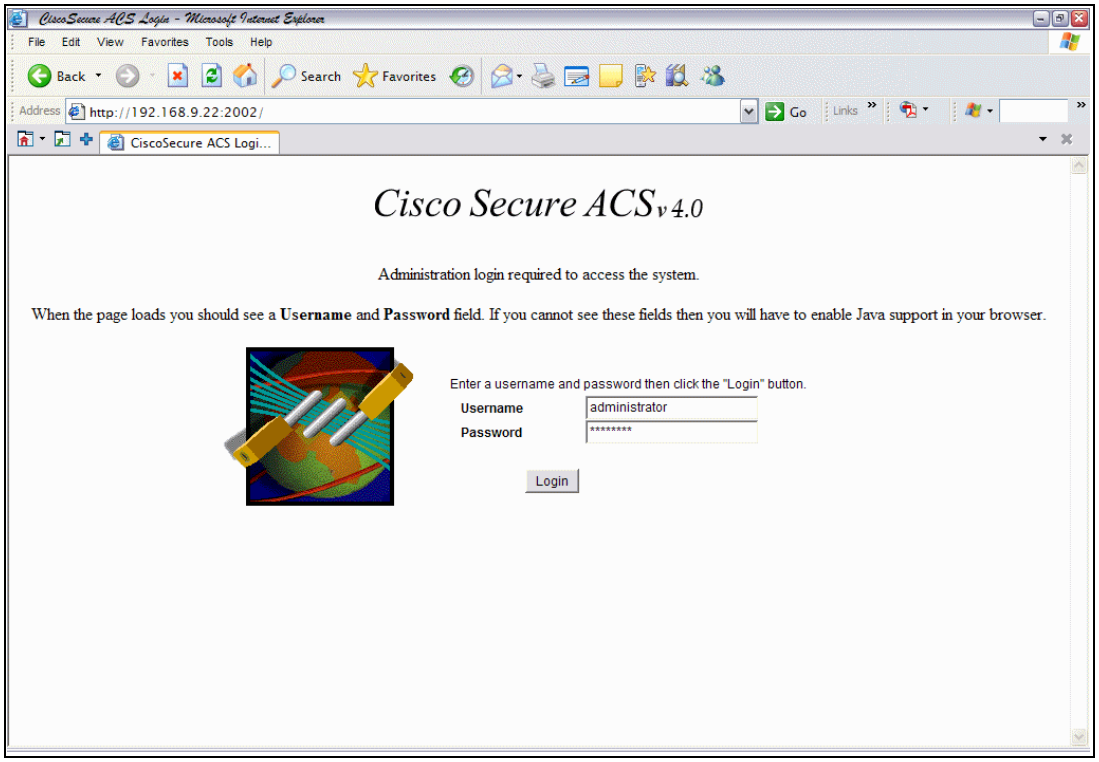

CiscoSecure ACS Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:2002/
Go Links
CiscoSecure ACS Logi...
Cisco Secure ACS v4.0
Administration login required to access the system.
When the page loads you should see a Username and Password field. If you cannot see these fields then you will have to enable Java support in your browser.
Enter a username and password then click the "Login" button.
Username
administrator
Password
****
Login

Figure 7-1 Cisco Secure ACS Welcome window

Downloaded from www.Manualslib.com manuals search engine

Configuring the administrative interface to Cisco Secure ACS

By default, not all features and options of the Cisco Secure ACS administrator interface are enabled. The advanced features required by the IBM Integrated Security Solution for Cisco Networks are not used in common Cisco Secure ACS deployments. For our solution some of these features must be activated. They are used by Cisco Secure ACS to communicate enforcement actions to the NAD.

To enable the appearance of the enforcement action interface in the Cisco Secure ACS administrator interface, perform the following steps:

1. Click **Interface Configuration** on the Cisco Secure ACS main menu.
2. Click **Advanced Options** (Figure 7-2) at the bottom of the list of options.

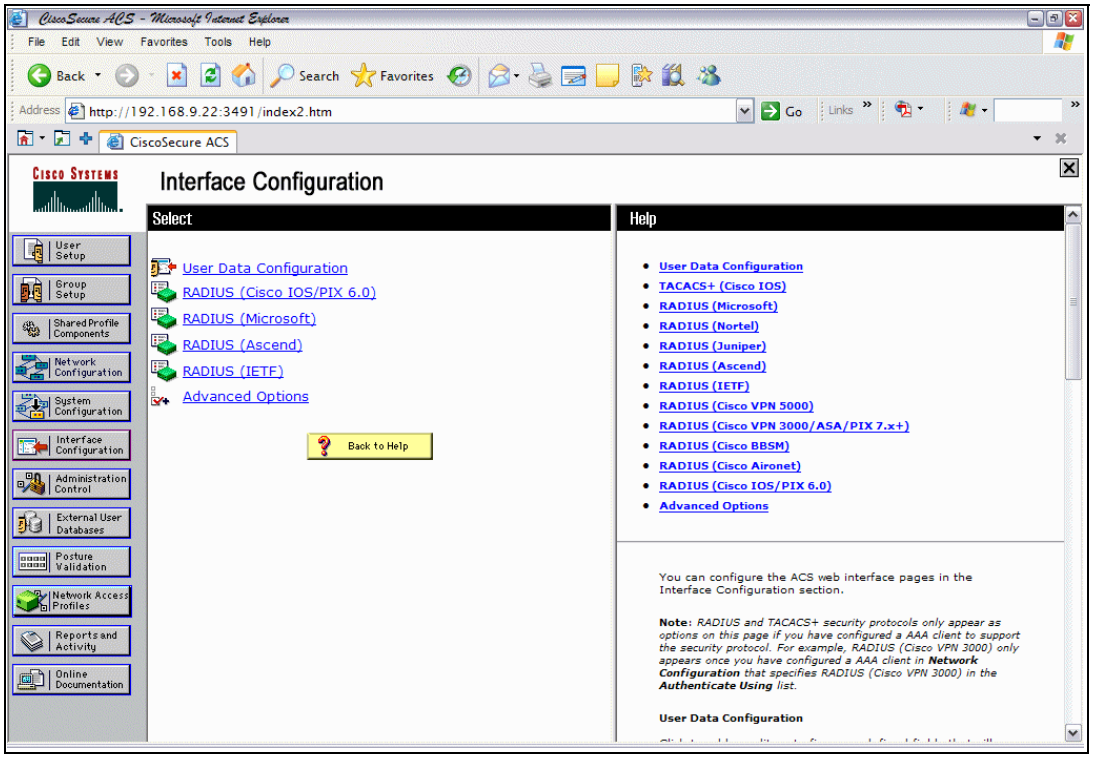

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3491/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
User Data Configuration
RADIUS (Cisco IOS/PIX 6.0)
RADIUS (Microsoft)
RADIUS (Ascend)
RADIUS (IETF)
Advanced Options
Back to Help
Help
User Data Configuration
TACACS+ (Cisco IOS)
RADIUS (Microsoft)
RADIUS (Nortel)
RADIUS (Juniper)
RADIUS (Ascend)
RADIUS (IETF)
RADIUS (Cisco VPN 5000)
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
RADIUS (Cisco BBSM)
RADIUS (Cisco Aironet)
RADIUS (Cisco IOS/PIX 6.0)
Advanced Options
You can configure the ACS web interface pages in the Interface Configuration section.
Note: RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000) in the Authenticate Using list.
User Data Configuration

Figure 7-2 Interface Configuration main menu

3. This opens the window in Figure 7-3 on page 217. Under **Advanced Options**, select:
   - Group-Level downloadable ACLs

     This enables the appearance of the downloadable ACLs option in the Shared Profile Components and Group Setup interfaces. These are used to cause Cisco Secure ACS to send dynamic access control lists to the NAD to be applied on a client undergoing NAC.

Downloaded from www.Manualslib.com manuals search engine

Note: Group-level downloadable ACLs are not yet supported for L2Dot1x. They are only supported for NAC L2/L3 IP. It is Cisco's stated intention that future releases of IOS for switches will support downloadable ACLs for NAC L2 802.1x. Access restriction for NAC L2 802.1x should be configured as an access-list bound to the SVI on the L3 device closest to the end user. In the example used for this book, the access lists were bound to the SVIs defined on the 3750 switch.

– Network Access Filtering

  This option enables the appearance of the network access filtering option under the Shared Profile Components window. This allows a network to have different enforcement policies downloaded for applications to a client in a particular state depending on where in the network the client is located. For instance, if multiple remediation servers are present in a network, it is best to send a client in a quarantined state to the closest remediation server for its software update.

4. Click **Submit** (Figure 7-3) to add these configuration options to the **Shared Profile Components** interface. These options are necessary for the configuration of the enforcement actions taken by the NAD.

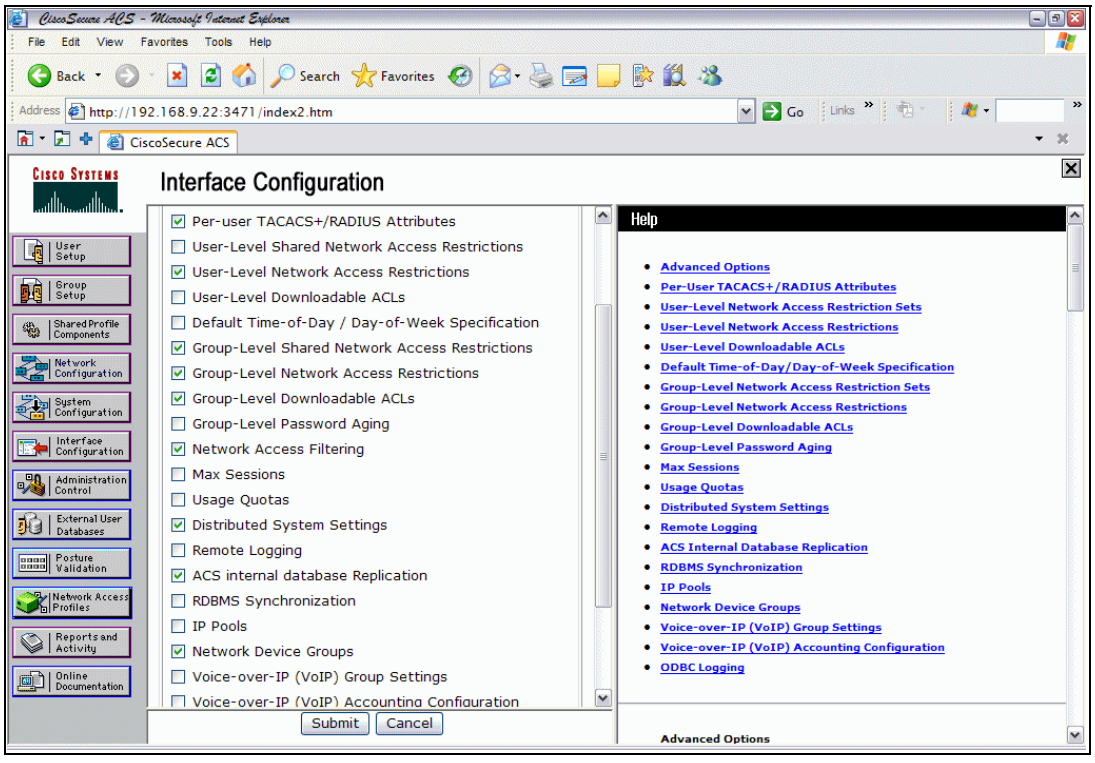


Figure 7-3 Interface configuration advanced options

Downloaded from www.Manualslib.com manuals search engine

Allowing administrator access via HTTP (optional)

If you want to configure ACS from a remote client using the Web interface, you must configure at least one administrator user name and password:

1. Click **Administration Control** on the Cisco Secure ACS main menu. This opens the window shown in Figure 7-4. Click **Add Administrator**.

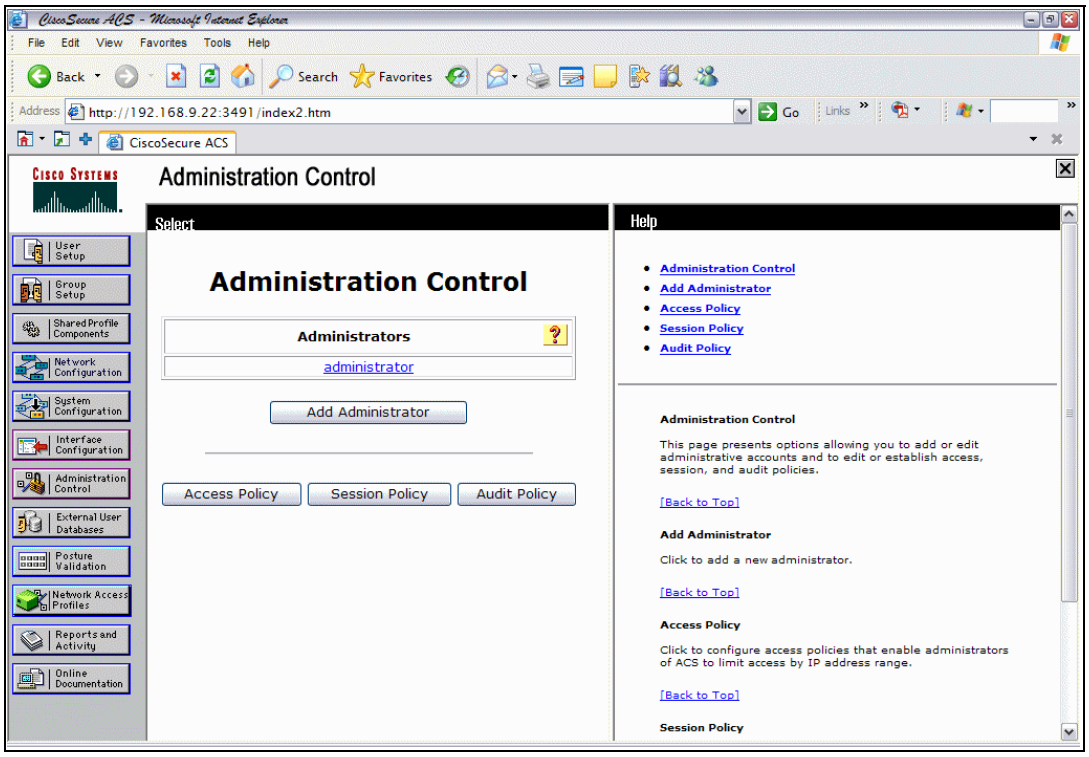


Figure 7-4 Administration control

Downloaded from www.Manualslib.com manuals search engine

2. Fill in the user name and password fields, and click **Grant All** to give all configuration rights to the administrator. If desired, an administrator's privileges can be limited to individual groups and components in order to have separate administrators for different parts of the network and network policies.

   Click **Submit** to complete the process.

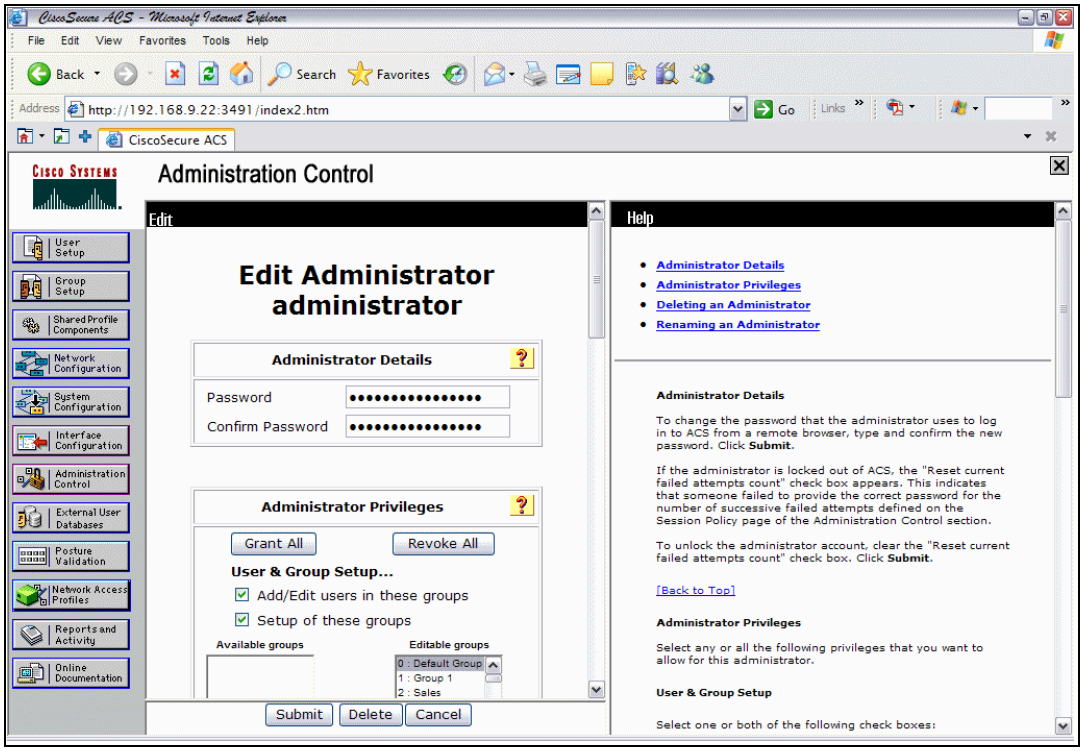

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3491/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Administration Control
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Edit Administrator
administrator
Administrator Details
Password
Confirm Password
Administrator Privileges
Grant All
Revoke All
User & Group Setup...
Add/Edit users in these groups
Setup of these groups
Available groups
Editable groups
0 : Default Group
1 : Group 1
2 : Sales
Submit
Delete
Cancel
Help
Administrator Details
Administrator Privileges
Deleting an Administrator
Renaming an Administrator
Administrator Details
To change the password that the administrator uses to log in to ACS from a remote browser, type and confirm the new password. Click Submit.
If the administrator is locked out of ACS, the "Reset current failed attempts count" check box appears. This indicates that someone failed to provide the correct password for the number of successive failed attempts defined on the Session Policy page of the Administration Control section.
To unlock the administrator account, clear the "Reset current failed attempts count" check box. Click Submit.
[Back to Top]
Administrator Privileges
Select any or all the following privileges that you want to allow for this administrator.
User & Group Setup
Select one or both of the following check boxes:

Figure 7-5 Administration privileges

Cisco Secure ACS certificate setup

ACS should be configured with a digital certificate for establishing client trust when challenging the client for its credentials. Cisco Secure ACS uses the X.509 v3 digital certificate standard. Certificate files must be in Base64-encoded X.509 format or Distinguished Encoding Rules (DER)-encoded binary X.509 format. Also, Cisco Secure ACS supports manual certificate enrollment and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRL). You must complete a certificate installation process and restart Cisco Secure ACS before beginning the PEAP configuration.

Downloaded from www.Manualslib.com manuals search engine

Note: We highly recommend that you use a production PKI and certificates signed by the production certificate authority (CA) or a registration authority (RA) for the most scalable NAC deployments. You will need to use an existing PKI (internal or outsourced) to securely identify the ACS infrastructure to endpoint devices (for example, CTA). For information about obtaining and installing a certificate from a certificate authority refer to (requires CCO login):

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_user_guide_chapter09186a008052e963.html

Cisco Secure ACS uses the certificate store that is built into the Windows operating system. The server certificate may be installed in several ways.

If you have an external public/private CA, you can add the CA to the local certificate storage on the ACS. After the certificate has been added, it must be enabled on the certificate trust list before it can be used to authenticate users.

Cisco Secure ACS Version 4.0 can also generate a self-signed certificate. A self-signed certificate is useful when no CA or other trust authority is required. In this case, the certificate from Cisco Secure ACS is installed on each client taking part in the network admission control process.

For the purpose of the book, we used a self-signed certificate.

Using an ACS self-signed certificate

With Cisco Secure ACS Version 4.0 you can generate a self-signed certificate, which is useful when no CA or other trust authority is required.

Downloaded from www.Manualslib.com manuals search engine

To use a self-signed certificate, perform the following steps:

1. Click **Generate Self-Signed Certificate** in the **Cisco Secure ACS Certificate Setup** window (Figure 7-6).

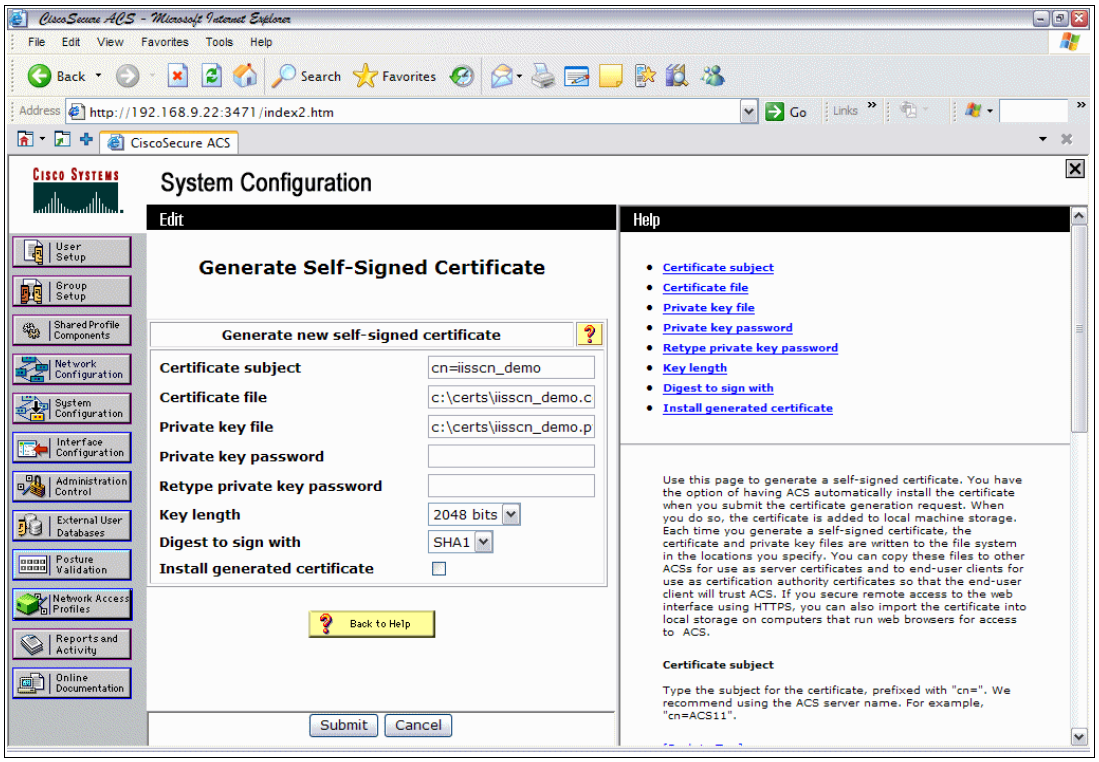

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3471/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
System Configuration
Edit
Help
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Generate Self-Signed Certificate
Generate new self-signed certificate
Certificate subject cn=iisscn_demo
Certificate file c:\certs\iisscn_demo.c
Private key file c:\certs\iisscn_demo.p
Private key password
Retype private key password
Key length 2048 bits
Digest to sign with SHA1
Install generated certificate
Back to Help
Submit Cancel
Certificate subject
Certificate file
Private key file
Private key password
Retype private key password
Key length
Digest to sign with
Install generated certificate
Use this page to generate a self-signed certificate. You have the option of having ACS automatically install the certificate when you submit the certificate generation request. When you do so, the certificate is added to local machine storage. Each time you generate a self-signed certificate, the certificate and private key files are written to the file system in the locations you specify. You can copy these files to other ACSs for use as server certificates and to end-user clients for use as certification authority certificates so that the end-user client will trust ACS. If you secure remote access to the web interface using HTTPS, you can also import the certificate into local storage on computers that run web browsers for access to ACS.
Certificate subject
Type the subject for the certificate, prefixed with "cn=". We recommend using the ACS server name. For example, "cn=ACS11".

Figure 7-6 Generating self-signed certificate

2. Fill in the blanks with the appropriate information according to your own installation. Be sure to enable *Install generated certificate*. In the example used here:
   - Certificate subject: cn=iisscn_demo
   - Certificate file: c:\certs\iisscn_demo.cer
   - Private key file: c:\certs\iisscn_demo.pvk
   - Key length: 2048 bits
   - Digest to sign with: SHA1
3. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

4. Restart the Cisco Secure ACS (Figure 7-7).

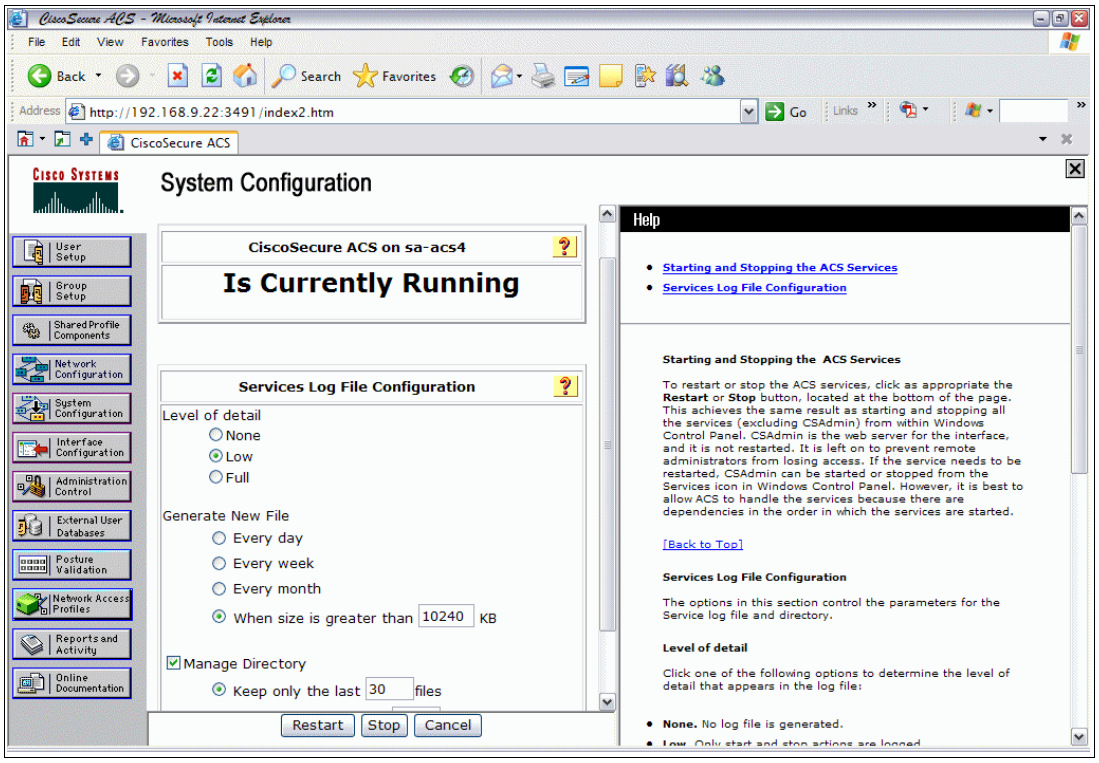

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3491/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
System Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
CiscoSecure ACS on sa-acs4
Is Currently Running
Services Log File Configuration
Level of detail
None
Low
Full
Generate New File
Every day
Every week
Every month
When size is greater than 10240 KB
Manage Directory
Keep only the last 30 files
Restart
Stop
Cancel
Help
Starting and Stopping the ACS Services
Services Log File Configuration
Starting and Stopping the ACS Services
To restart or stop the ACS services, click as appropriate the Restart or Stop button, located at the bottom of the page. This achieves the same result as starting and stopping all the services (excluding CSAdmin) from within Windows Control Panel. CSAdmin is the web server for the interface, and it is not restarted. It is left on to prevent remote administrators from losing access. If the service needs to be restarted, CSAdmin can be started or stopped from the Services icon in Windows Control Panel. However, it is best to allow ACS to handle the services because there are dependencies in the order in which the services are started.
[Back to Top]
Services Log File Configuration
The options in this section control the parameters for the Service log file and directory.
Level of detail
Click one of the following options to determine the level of detail that appears in the log file:
None. No log file is generated.

Figure 7-7 Restart Cisco Secure ACS

Downloaded from www.Manualslib.com manuals search engine

5. After completing the certificate setup process and installation, verify that the certificate has been installed by clicking **Install ACS Certificate** from the **ACS Certificate Setup** screen (Figure 7-8).

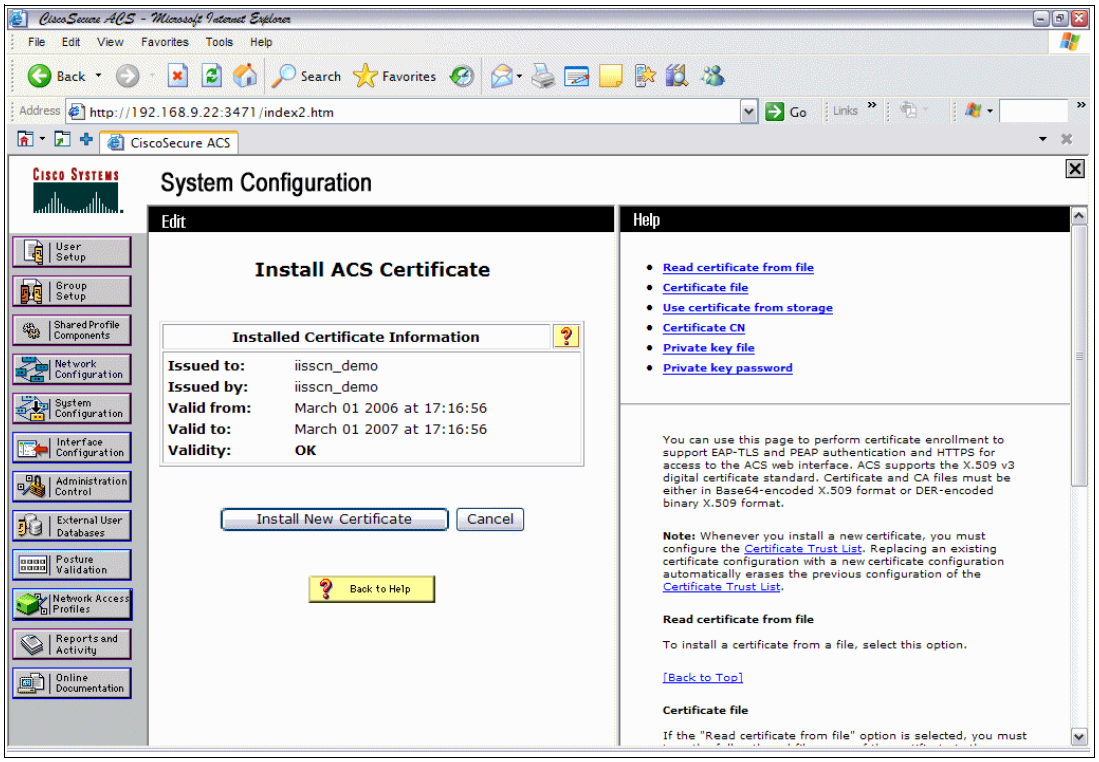


Figure 7-8 Self-signed certificate installation verification

6. After generating and installing the self-signed certificate on the Cisco Secure ACS, include the certificate file as part of the install process for each client when installing the Cisco Trust Agent, or install the certificate file manually using ctaCert.exe on each client.

Importing IBM Security Compliance Manager attributes

New Security Compliance Manager attributes must be imported to the Cisco Secure ACS. This enables these new attributes to be utilized as part of the ACS policy rules checking as well as the ACS logging subsystem.

Downloaded from www.Manualslib.com manuals search engine

To import Security Compliance Manager attributes, perform the following steps:

1. Copy the Security Compliance Manager attributes definition file to a directory accessible to the Cisco Secure ACS. Example 7-1 shows the content of the Security Compliance Manager attribute definition file for information purposes. We strongly urge you not to modify this file.

Example 7-1 Security Compliance Manager attributes

```
[attr#0]
vendor-id=2
vendor-name=IBM Corporation
application-id=50
application-name=SCM
attribute-id=00020
attribute-name=Policy Version
attribute-profile=in out
attribute-type=string
[attr#1]
vendor-id=2
vendor-name=IBM Corporation
application-id=50
application-name=SCM
attribute-id=00021
attribute-name=Violation count
attribute-profile=in out
attribute-type=unsigned integer
[attr#2]
vendor-id=2
vendor-name=IBM Corporation
application-id=50
application-name=SCM
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=String
```

2. Open a command prompt and change to the directory containing CSUtil.exe. If you install Cisco Secure ACS in the default location, the CSUtil.exe is located in the C:\Program Files\CiscoSecure ACS v4.0\Utils directory.
3. Add the Security Compliance Manager attributes to ACS by running:

```
csutil.exe -addavp filename
```


Downloaded from www.Manualslib.com manuals search engine

filename is the name of the file in which you want CSUtil.exe to write all attribute definitions. Example 7-2 shows the execution of this command.

Example 7-2 Import Security Compliance Manager attribute

```
C:\Program Files\CiscoSecure ACS v4.0\Utils>CSUtil -addavp
c:\Temp\avplist.txt

Attribute 2:50:1 (Application-Posture-Token) automatically added to
registry
Attribute 2:50:2 (System-Posture-Token) automatically added to registry

[attr#0]: Attribute 2:50:10 (Action) added to registry
[attr#1]: Attribute 2:50:20 (Policy Version) added to registry
[attr#2]: Attribute 2:50:21 (Violation number) added to registry

=== AVP Summary ===
3 AVPs were added to the registry

In addition, 2 AVPs were automatically added to the registry

=== IMPORTANT NOTICE ===
Please restart the following services:
- CSAdmin
- CSAuth
- CSLog

C:\Program Files\CiscoSecureACS v4.0\Utils>
```

4. To make the Security Compliance Manager attribute definitions take effect, restart the CSAuth, CSLog, and CSAdmin services by entering the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth

net start csauth

net stop cslog

net start cslog

net stop csadmin

net start csadmin
```

5. ACS should now be aware of the Security Compliance Manager attributes. To verify this, run the command:

```
csutil.exe –dumpavp filename
```


Downloaded from www.Manualslib.com manuals search engine

filename is the file that the attributes will be written to. The Security Compliance Manager attributes should be viewable in this file.

Tip: The result of **`csutil.exe -dumpavp`** contains these two attributes, which are added automatically when **`csutil.exe -addavp`** is executed:

- IBM Corporation:SCM:Application-Posture-Token
- IBM Corporation:SCM:System-Posture-Token

Configuring logging

Logging configuration is crucial for monitoring, reporting, and troubleshooting a NAC implementation.

To set up logging:

1. Click **System Configuration** on the Cisco Secure ACS main menu.
2. Click **Logging**.
3. Click **CSV Passed Authentications** (Figure 7-9).

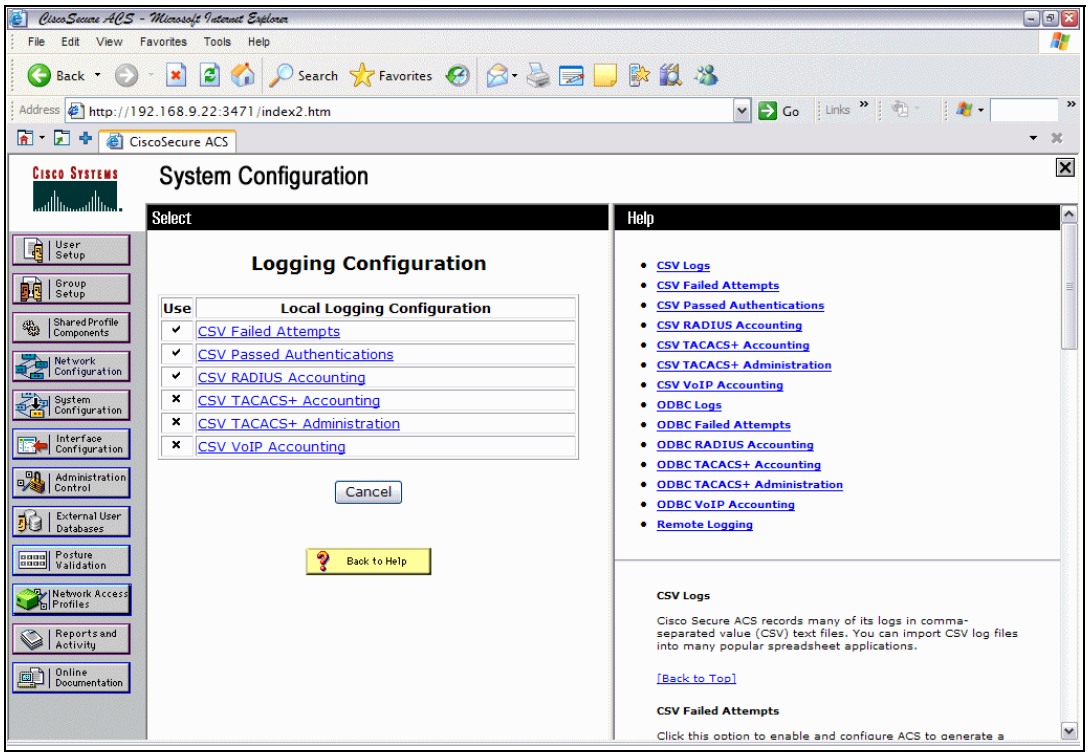


Figure 7-9 Logging configuration

4. Enable the Log to CSV Passed Authentications report (Figure 7-10 on page 227) and in the Select Columns To Log list, select the attributes (fields)

Downloaded from www.Manualslib.com manuals search engine

that you wish to include in the log file. Scroll down and change the file management settings if desired.

We recommend that you include the following fields in Logged Attribute:

- Network Access Profile Name
- Shared RAC
- Application Posture Token
- System Posture Token
- Reason

These should be moved toward the top of the list of installed attributes for easy access. This makes writing policy rules and troubleshooting much easier. The *NAS-IP-Address* and *User Name* fields also provide valuable information during troubleshooting.

All client instances successfully completing the posture validation process are logged in the passed authentications log even if the client has posture validated into a state other than Healthy. The failed authentication attempts log contains entries for clients failing to complete the posture validation process.

When you are finished, click **Submit**.

5. Select **CSV Failed Authentications** (Figure 7-10).

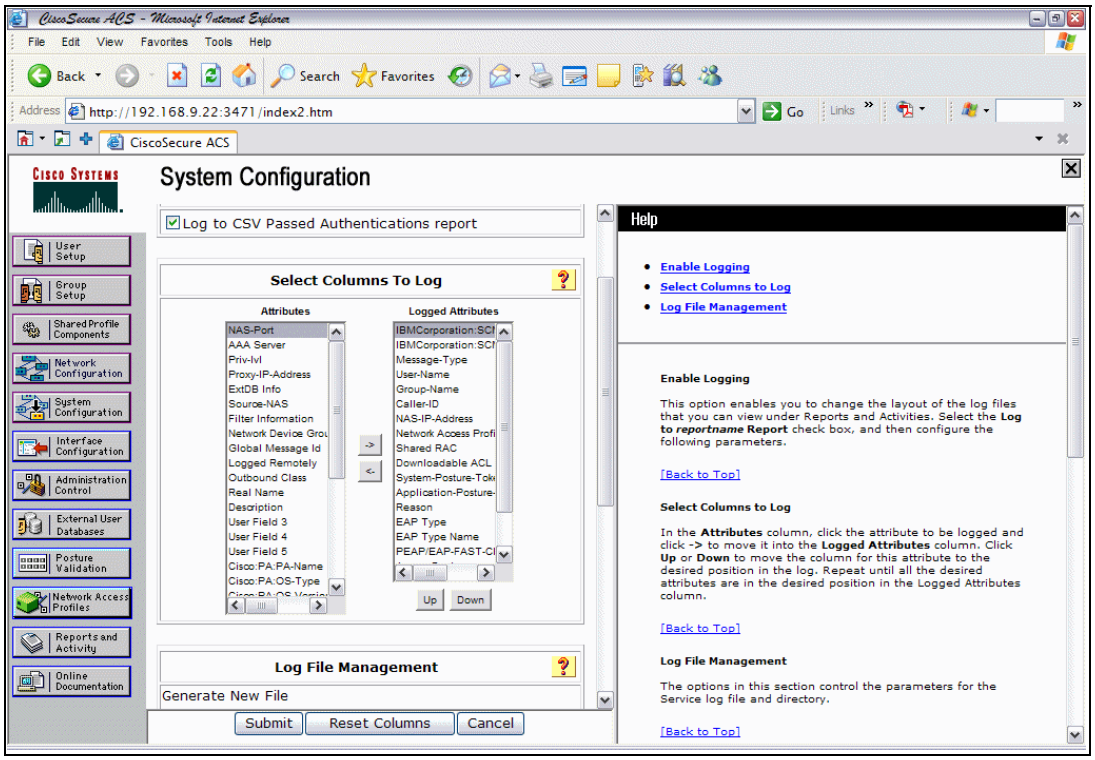


Figure 7-10 Passed authentication logging

Downloaded from www.Manualslib.com manuals search engine

6. Click the **Log to CSV Failed Attempts** report under Enable Logging. Repeat step 4 on page 226, selecting the items you wish to log. A selection is shown in Figure 7-11.

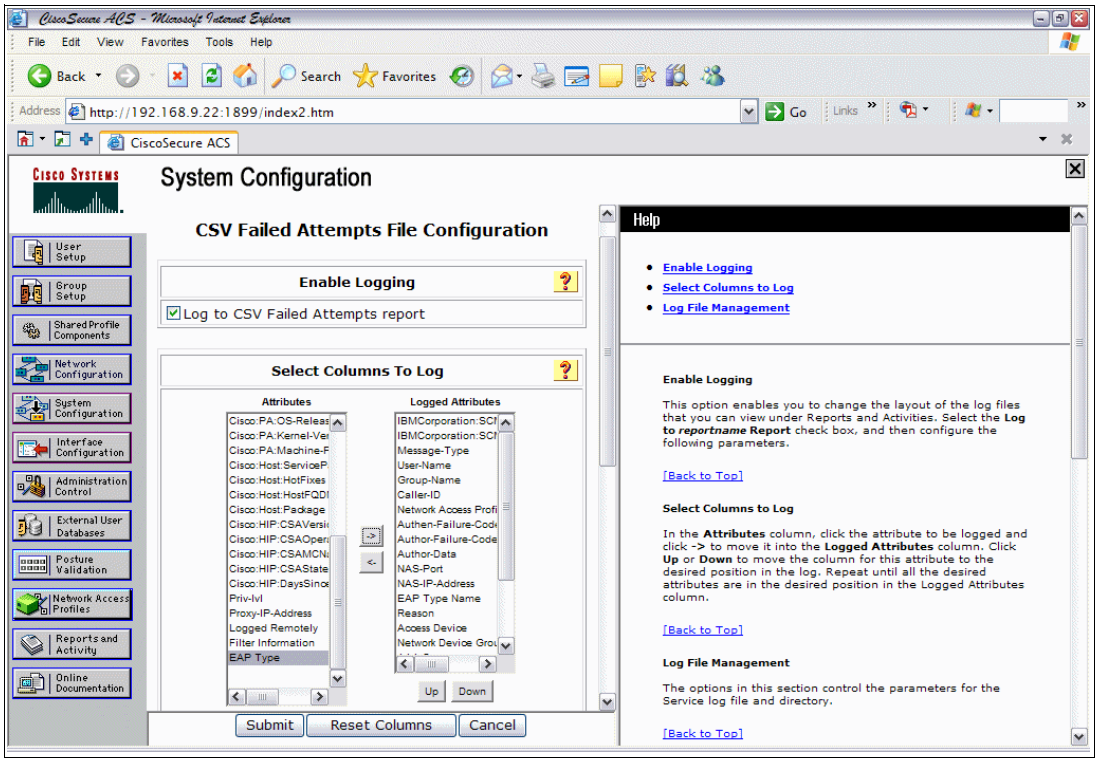


Figure 7-11 Failed attempts logging

7. Click **System Configuration** again on the Cisco Secure ACS main menu, and click **Service Control**.

Downloaded from www.Manualslib.com manuals search engine

8. In the window in under Services Log File Configuration (Figure 7-12) change Level of Detail to **Full**, and increase the file size from 2048 Kb as necessary. Click **Restart** to apply the new configuration.

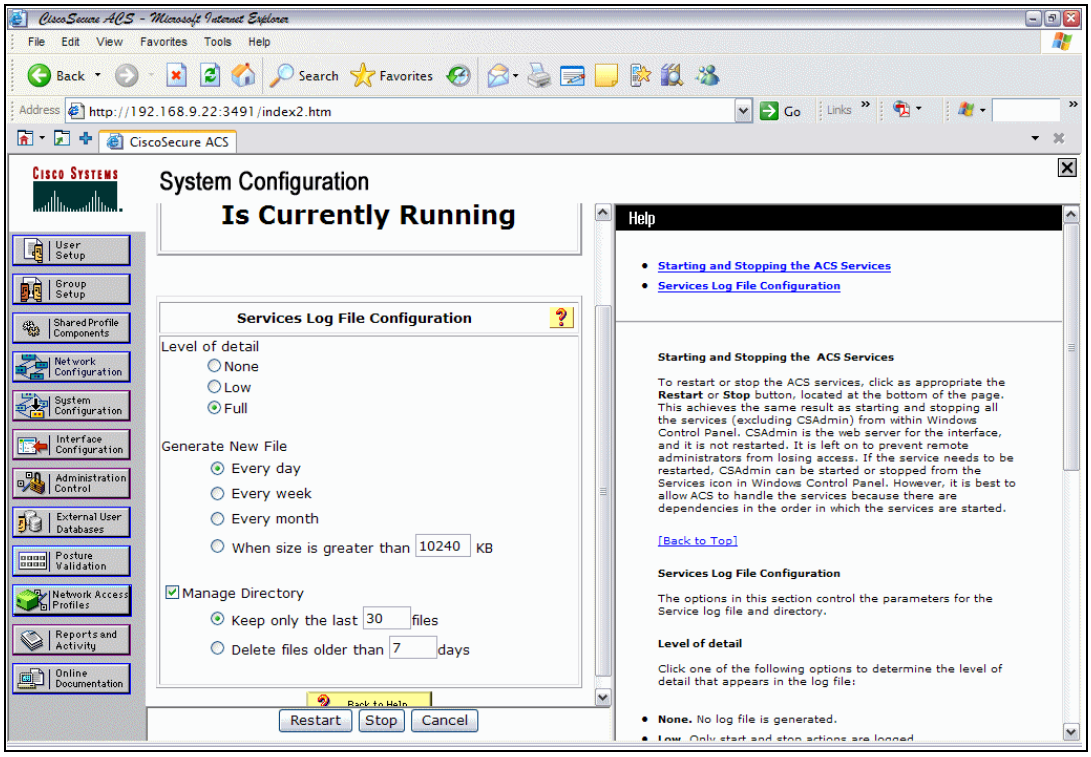

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3491/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
System Configuration
Is Currently Running
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Services Log File Configuration
Level of detail
None
Low
Full
Generate New File
Every day
Every week
Every month
When size is greater than 10240 KB
Manage Directory
Keep only the last 30 files
Delete files older than 7 days
Restart
Stop
Cancel
Help
Starting and Stopping the ACS Services
Services Log File Configuration
Starting and Stopping the ACS Services
To restart or stop the ACS services, click as appropriate the Restart or Stop button, located at the bottom of the page. This achieves the same result as starting and stopping all the services (excluding CSAdmin) from within Windows Control Panel. CSAdmin is the web server for the interface, and it is not restarted. It is left on to prevent remote administrators from losing access. If the service needs to be restarted, CSAdmin can be started or stopped from the Services icon in Windows Control Panel. However, it is best to allow ACS to handle the services because there are dependencies in the order in which the services are started.
[Back to Top]
Services Log File Configuration
The options in this section control the parameters for the Service log file and directory.
Level of detail
Click one of the following options to determine the level of detail that appears in the log file:
None. No log file is generated.

Figure 7-12 Log file management

Configuring a network device group in Cisco Secure ACS

To make Cisco Secure ACS interact with a Network Access Device (router, switch, VPN concentrator, and so on), you must configure Cisco Secure ACS to use the proper NAD information. In Cisco Secure ACS, a NAD is recognized as an authentication, authorization, accounting (AAA) client.

Downloaded from www.Manualslib.com manuals search engine

It is possible to group the NADs into Network Device Groups (NDGs) for location or service-based filtering. To do this, the use of NDGs must first be enabled:

1. Click **Interface Configuration** from the main menu (Figure 7-13).

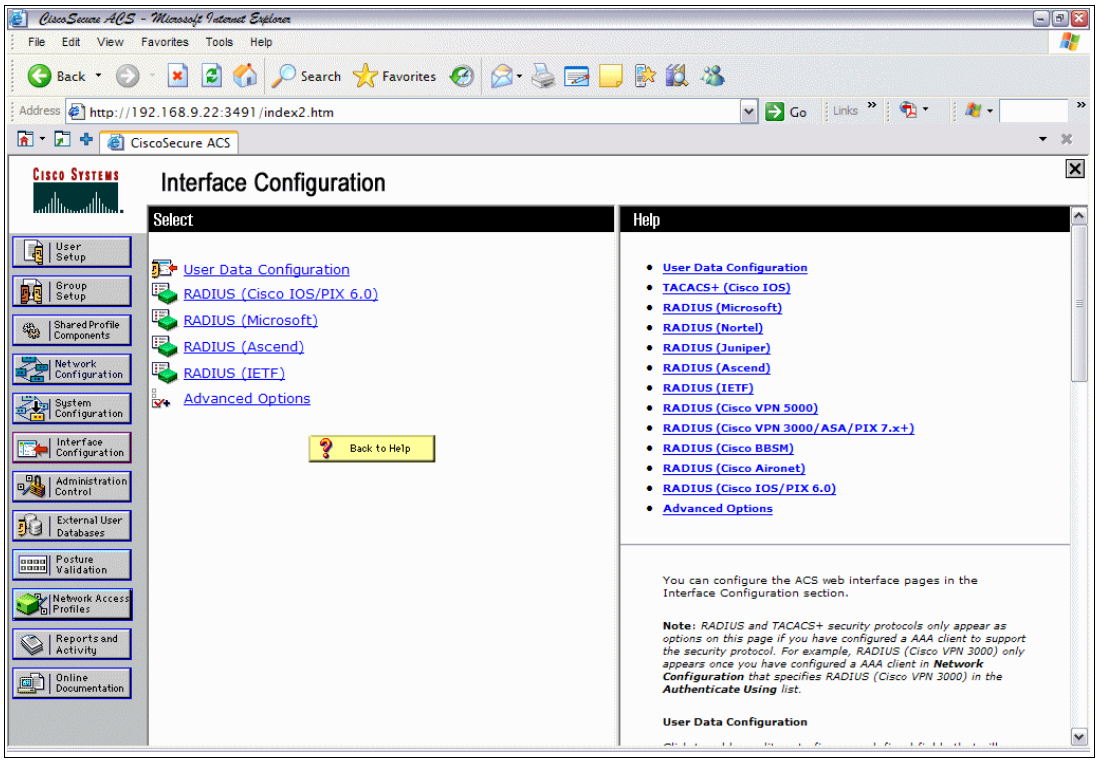

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3491/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
User Data Configuration
RADIUS (Cisco IOS/PIX 6.0)
RADIUS (Microsoft)
RADIUS (Ascend)
RADIUS (IETF)
Advanced Options
Back to Help
Help
User Data Configuration
TACACS+ (Cisco IOS)
RADIUS (Microsoft)
RADIUS (Nortel)
RADIUS (Juniper)
RADIUS (Ascend)
RADIUS (IETF)
RADIUS (Cisco VPN 5000)
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
RADIUS (Cisco BBSM)
RADIUS (Cisco Aironet)
RADIUS (Cisco IOS/PIX 6.0)
Advanced Options
You can configure the ACS web interface pages in the Interface Configuration section.
Note: RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000) in the Authenticate Using list.
User Data Configuration

Figure 7-13 Interface Configuration screen for the creation of NDGs

Downloaded from www.Manualslib.com manuals search engine

2. Select **Advanced Options** (Figure 7-13 on page 230). Ensure that **Network Device Groups** is checked (Figure 7-14).

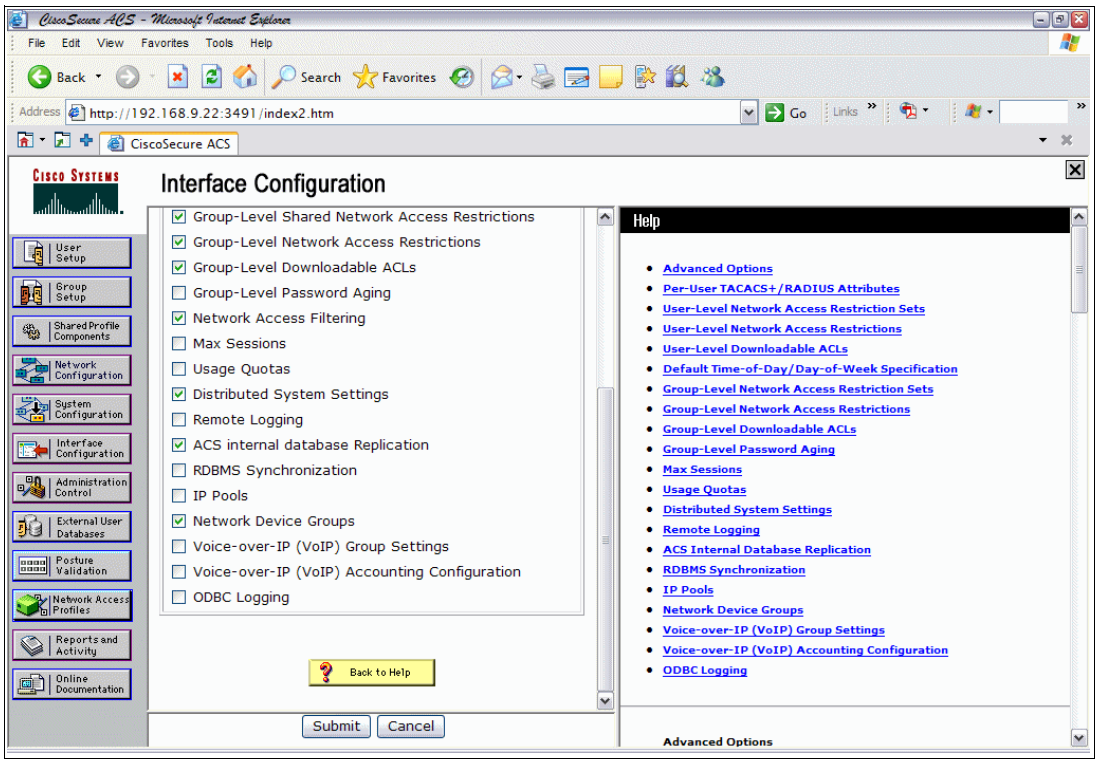


Figure 7-14 Network Device Group check box

Downloaded from www.Manualslib.com manuals search engine

3. Select **Network Configuration** in the main menu. The screen in Figure 7-15 is shown.

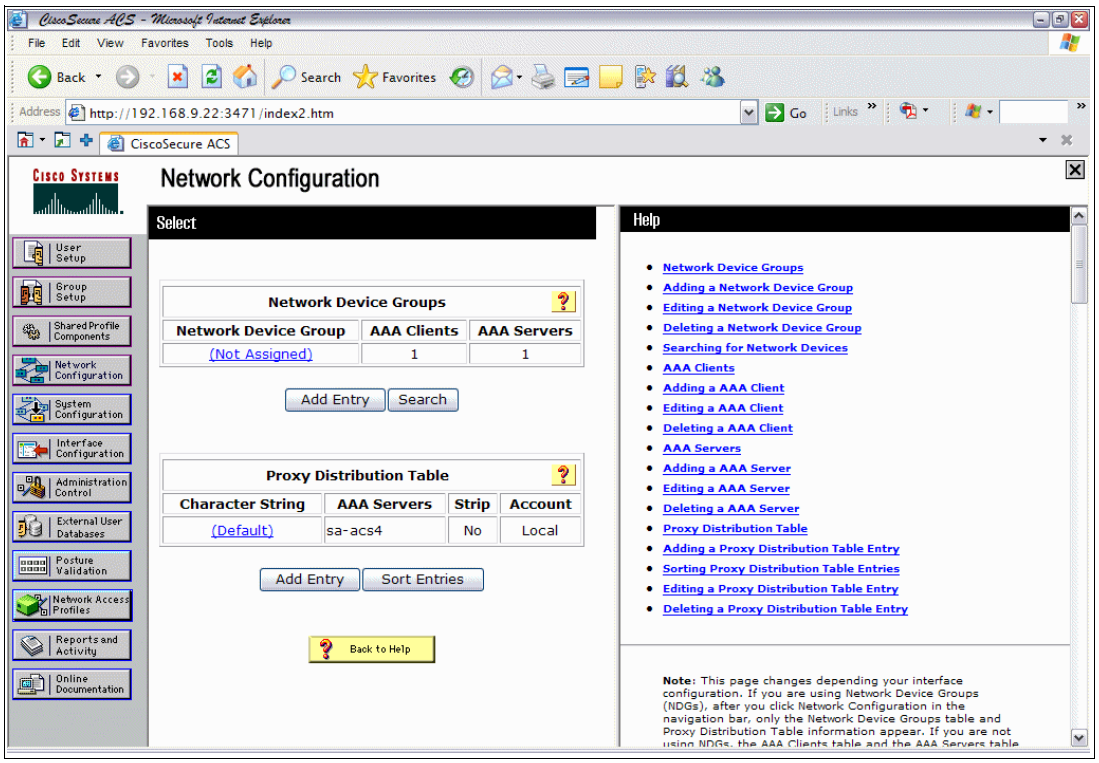


Figure 7-15 Network Configuration

> **Note:** Figure 7-15 changes depending on your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the main menu, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

4. (Optional) Select **Add Entry** under Network Device Groups (Figure 7-15).
5. (Optional) Add the name of the NDG you wish to use (for example, switches) and the RADIUS key used by the AAA clients that makes up this NDG (for example, cisco123).

Downloaded from www.Manualslib.com manuals search engine

6. From the Network Configuration screen, select the hyperlink under Network Device Groups. If you did not assign a name in step 5, you will see `Not Assigned` as the name (Figure 7-15 on page 232). By clicking this link, you will see the AAA Clients (Figure 7-16).

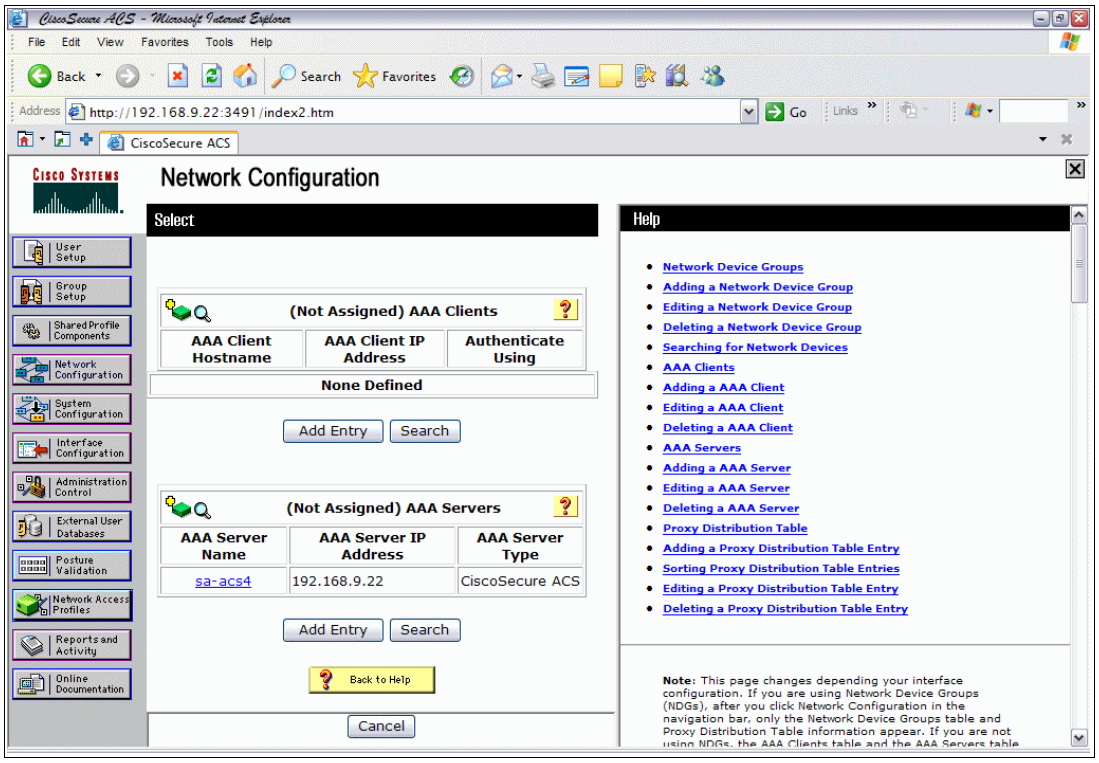


Figure 7-16 AAA clients

Downloaded from www.Manualslib.com manuals search engine

7. Click **Add Entry** under AAA Clients to add any AAA clients to this particular NDG. You can configure all NADs as a single AAA client by using IP address wild cards (*.*.*.*). In Figure 7-17 we have done this and used the RADIUS key cisco123. Note that authentication is done using RADIUS (IOS/PIX6.0). There are other options available, depending on what is being defined as a NAD. Click **Submit** and then **Apply**.

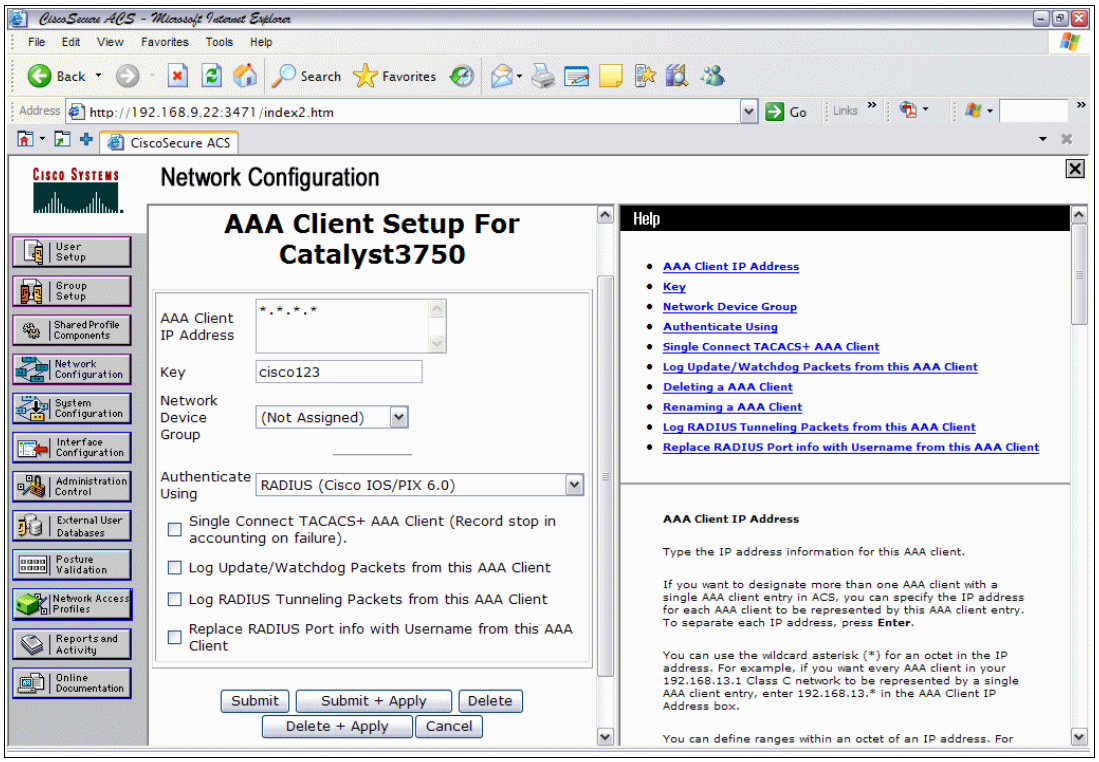

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3471/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
AAA Client Setup For Catalyst3750
AAA Client IP Address
..*.*
Key
cisco123
Network Device Group
(Not Assigned)
Authenticate Using
RADIUS (Cisco IOS/PIX 6.0)
Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Log Update/Watchdog Packets from this AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Replace RADIUS Port info with Username from this AAA Client
Submit
Submit + Apply
Delete
Delete + Apply
Cancel
Help
AAA Client IP Address
Key
Network Device Group
Authenticate Using
Single Connect TACACS+ AAA Client
Log Update/Watchdog Packets from this AAA Client
Deleting a AAA Client
Renaming a AAA Client
Log RADIUS Tunneling Packets from this AAA Client
Replace RADIUS Port info with Username from this AAA Client
AAA Client IP Address
Type the IP address information for this AAA client.
If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.
You can define ranges within an octet of an IP address. For

Figure 7-17 AAA client setup

Note: The use of wild cards (*.*.*.*) is designed to help with scalability issues. For example, if your network has over 100 switches, defining each one as a separate NAD is very time consuming. By using *.*.*.*, all devices that are configured to point to the ACS as the RADIUS Server and have the same RADIUS key will exchange information with the ACS. This can provide a security vulnerability, however, if someone knows the RADIUS Server IP address and RADIUS key. A better option may be to define NDGs based on subnet information, such as 192.168.10.*, which will retain some scalability and security.

Downloaded from www.Manualslib.com manuals search engine

8. You should now see the newly defined AAA clients (Figure 7-18).

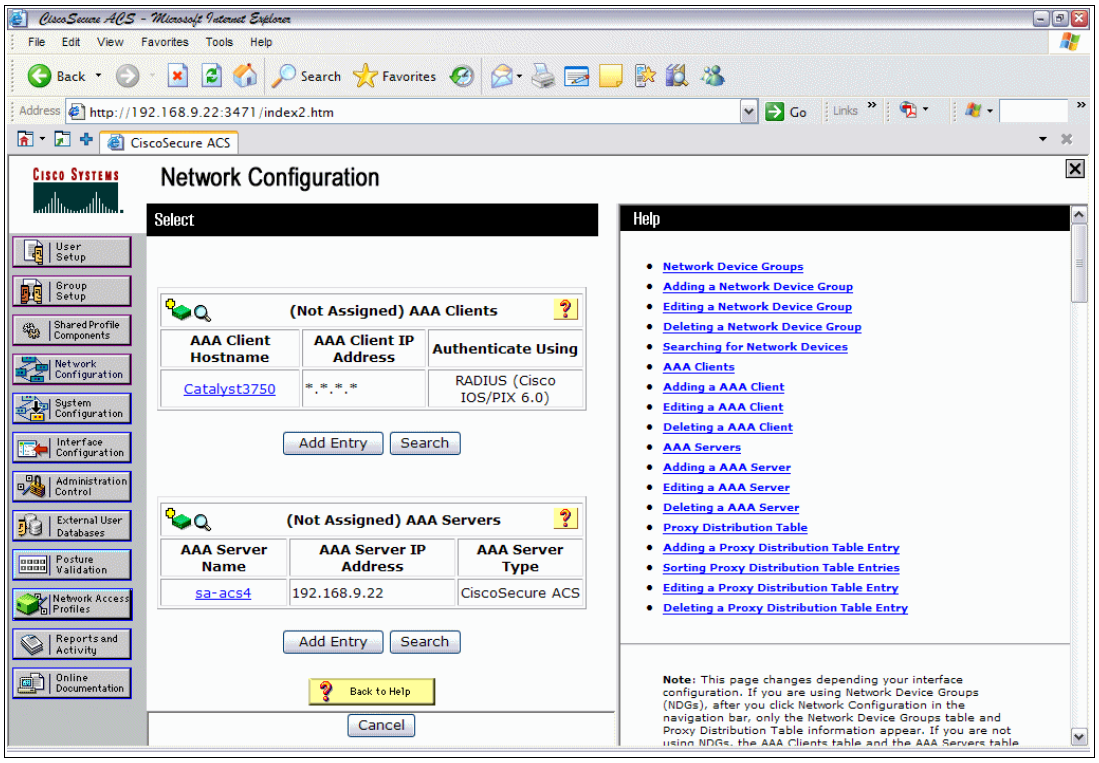


Figure 7-18 AAA Clients

Downloaded from www.Manualslib.com manuals search engine

Configuring RADIUS attributes

The RADIUS attributes required for NAC must be globally enabled on the Cisco Secure ACS.

1. Select **Interface Configuration** from the main menu (Figure 7-13 on page 230), then select **RADIUS (IETF)** (Figure 7-19).

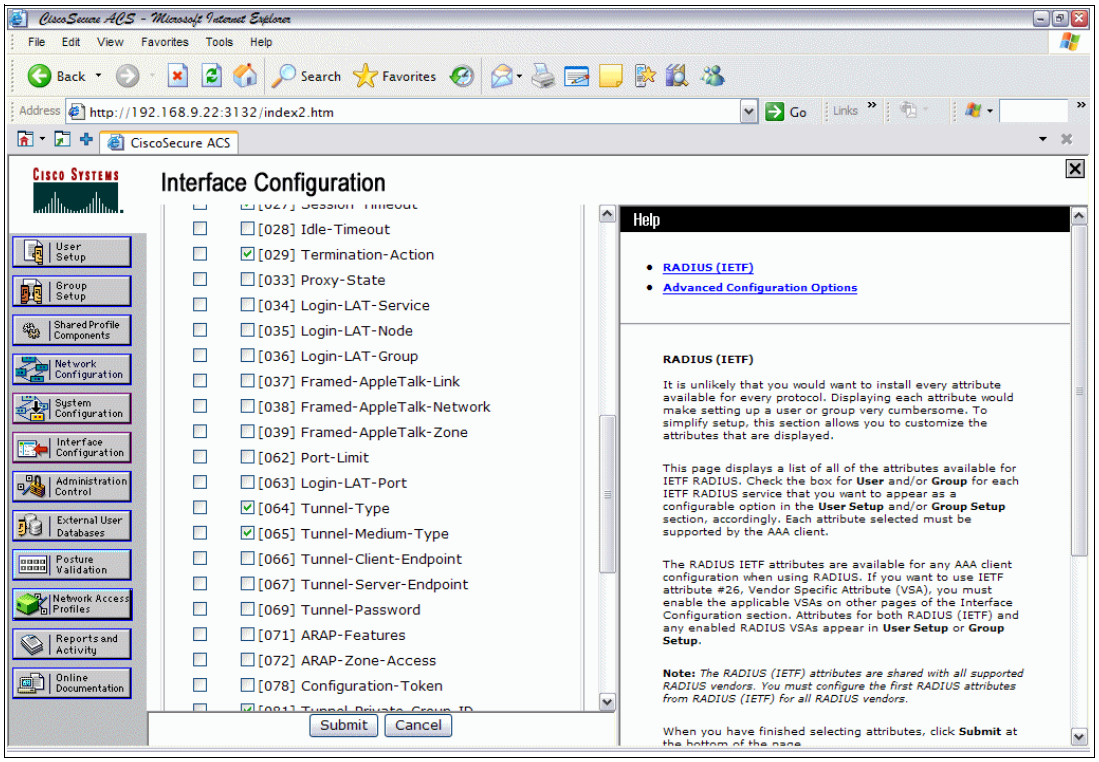

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3132/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[028] Idle-Timeout
[029] Termination-Action
[033] Proxy-State
[034] Login-LAT-Service
[035] Login-LAT-Node
[036] Login-LAT-Group
[037] Framed-AppleTalk-Link
[038] Framed-AppleTalk-Network
[039] Framed-AppleTalk-Zone
[062] Port-Limit
[063] Login-LAT-Port
[064] Tunnel-Type
[065] Tunnel-Medium-Type
[066] Tunnel-Client-Endpoint
[067] Tunnel-Server-Endpoint
[069] Tunnel-Password
[071] ARAP-Features
[072] ARAP-Zone-Access
[078] Configuration-Token
Submit
Cancel
Help
RADIUS (IETF)
Advanced Configuration Options
RADIUS (IETF)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each attribute would make setting up a user or group very cumbersome. To simplify setup, this section allows you to customize the attributes that are displayed.
This page displays a list of all of the attributes available for IETF RADIUS. Check the box for User and/or Group for each IETF RADIUS service that you want to appear as a configurable option in the User Setup and/or Group Setup section, accordingly. Each attribute selected must be supported by the AAA client.
The RADIUS IETF attributes are available for any AAA client configuration when using RADIUS. If you want to use IETF attribute #26, Vendor Specific Attribute (VSA), you must enable the applicable VSAs on other pages of the Interface Configuration section. Attributes for both RADIUS (IETF) and any enabled RADIUS VSAs appear in User Setup or Group Setup.
Note: The RADIUS (IETF) attributes are shared with all supported RADIUS vendors. You must configure the first RADIUS attributes from RADIUS (IETF) for all RADIUS vendors.
When you have finished selecting attributes, click Submit at

Figure 7-19 Global IETF RADIUS attributes

For L2Dot1x NAC, you must select the following:

- [027] Session-Timeout
- [029] Termination-Action
- [064] Tunnel-type
- [065] Tunnel-Medium-Type
- [081] Tunnel-Private-Group-ID

After selecting just these items, click **Submit**. This will take you back to the screen shown in Figure 7-13 on page 230.

Note: 64, 65, and 81 are required for VLAN assignment.

Downloaded from www.Manualslib.com manuals search engine

2. From the Interface Configuration menu, select **RADIUS (Cisco IOS/PIX 6.0)** (Figure 7-20).

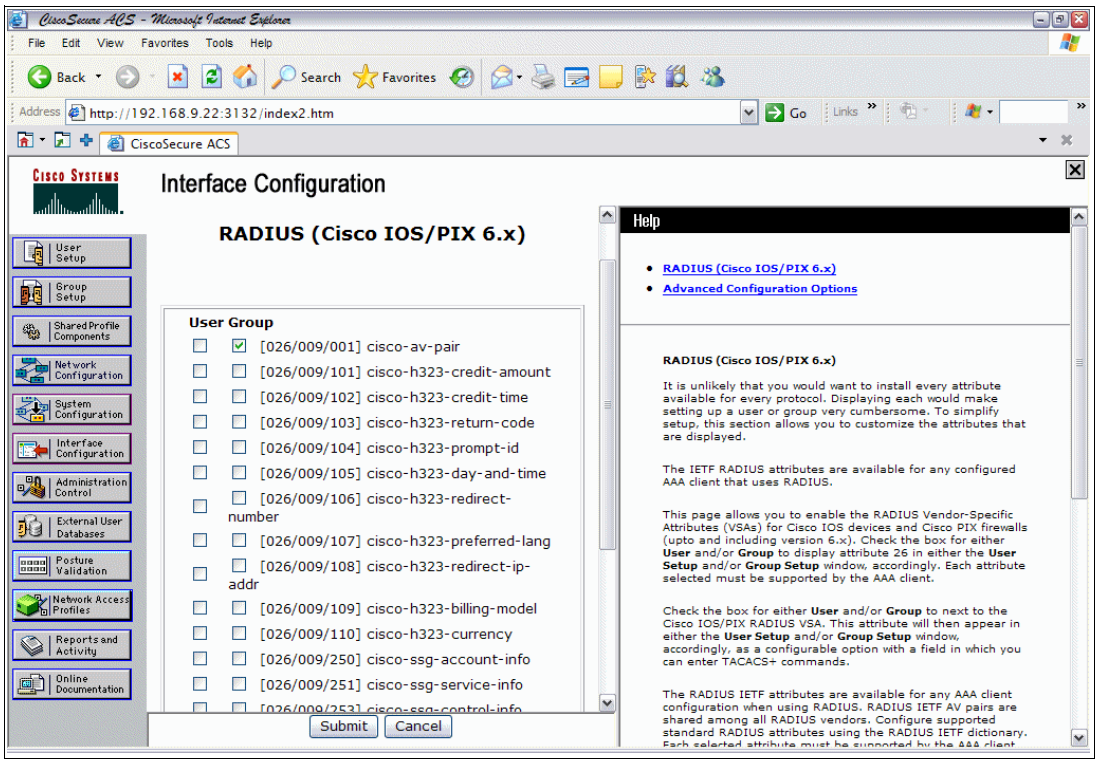

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3132/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Interface Configuration
RADIUS (Cisco IOS/PIX 6.x)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User Group
[026/009/001] cisco-av-pair
[026/009/101] cisco-h323-credit-amount
[026/009/102] cisco-h323-credit-time
[026/009/103] cisco-h323-return-code
[026/009/104] cisco-h323-prompt-id
[026/009/105] cisco-h323-day-and-time
[026/009/106] cisco-h323-redirect-number
[026/009/107] cisco-h323-preferred-lang
[026/009/108] cisco-h323-redirect-ip-addr
[026/009/109] cisco-h323-billing-model
[026/009/110] cisco-h323-currency
[026/009/250] cisco-ssg-account-info
[026/009/251] cisco-ssg-service-info
Submit
Cancel
Help
RADIUS (Cisco IOS/PIX 6.x)
Advanced Configuration Options
RADIUS (Cisco IOS/PIX 6.x)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group very cumbersome. To simplify setup, this section allows you to customize the attributes that are displayed.
The IETF RADIUS attributes are available for any configured AAA client that uses RADIUS.
This page allows you to enable the RADIUS Vendor-Specific Attributes (VSAs) for Cisco IOS devices and Cisco PIX firewalls (upto and including version 6.x). Check the box for either User and/or Group to display attribute 26 in either the User Setup and/or Group Setup window, accordingly. Each attribute selected must be supported by the AAA client.
Check the box for either User and/or Group to next to the Cisco IOS/PIX RADIUS VSA. This attribute will then appear in either the User Setup and/or Group Setup window, accordingly, as a configurable option with a field in which you can enter TACACS+ commands.
The RADIUS IETF attributes are available for any AAA client configuration when using RADIUS. RADIUS IETF AV pairs are shared among all RADIUS vendors. Configure supported standard RADIUS attributes using the RADIUS IETF dictionary.

Figure 7-20 Cisco IOS/PIX 6.0 RADIUS attributes

For L2Dot1x NAC, you must select [026/009/001] cisco-av-pair.

3. After selecting this item, click **Submit**.

Configuring groups

The group setup and configuration portion of the Cisco Secure ACS requires careful thought and planning. In the NAC L2 802.1x scenario we are using here, we have two locally defined groups, sales and engineering. One of the nice features about NAC L2 802.1x is the ability to place users into various different VLANS dynamically based on dot1x authentication and posture validation. In our scenario, the default VLAN for sales is VLAN 11. The default VLAN for engineering is VLAN 12. Part of the planning process is whether your groups will be locally defined on the Cisco Secure ACS, or will be mapped to a Microsoft

Downloaded from www.Manualslib.com manuals search engine

Active Directory, for example. To configure groups and vendor-specific attributes, complete these steps:

1. Click **Group Setup** on the Cisco Secure ACS Main Menu.
2. Choose any unused groups, and rename each group as applicable. In the example here, we have renamed Group 2 as Sales and Group 3 as Engineering.

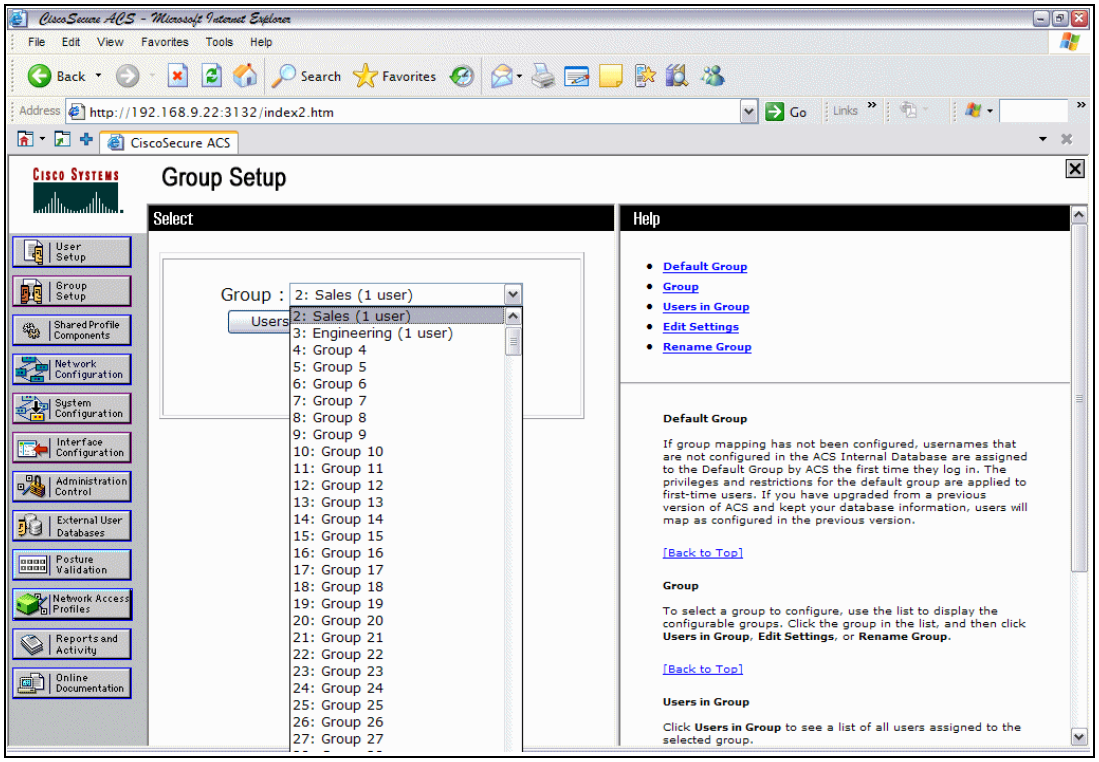

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3132/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Group Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
Group : 2: Sales (1 user)
Users
2: Sales (1 user)
3: Engineering (1 user)
4: Group 4
5: Group 5
6: Group 6
7: Group 7
8: Group 8
9: Group 9
10: Group 10
11: Group 11
12: Group 12
13: Group 13
14: Group 14
15: Group 15
16: Group 16
17: Group 17
18: Group 18
19: Group 19
20: Group 20
21: Group 21
22: Group 22
23: Group 23
24: Group 24
25: Group 25
26: Group 26
27: Group 27
Help
Default Group
Group
Users in Group
Edit Settings
Rename Group
Default Group
If group mapping has not been configured, usernames that are not configured in the ACS Internal Database are assigned to the Default Group by ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, users will map as configured in the previous version.
[Back to Top]
Group
To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click Users in Group, Edit Settings, or Rename Group.
[Back to Top]
Users in Group
Click Users in Group to see a list of all users assigned to the selected group.

Figure 7-21 Group Setup

> **Note:** Only the group names need to be defined. Once the RADIUS Authorization Components have been configured, they will be bound to the groups created here based on authentication and posture validation. This is where the VLAN assignments and RADIUS attributes for the groups are defined.

3. Click **Submit + Restart** after completing the group configuration.

Downloaded from www.Manualslib.com manuals search engine

Configuring users

Now that the groups have been defined, we can create our users and then add them to their relevant group.

1. From the main menu select **User Setup**, as shown in Figure 7-22.

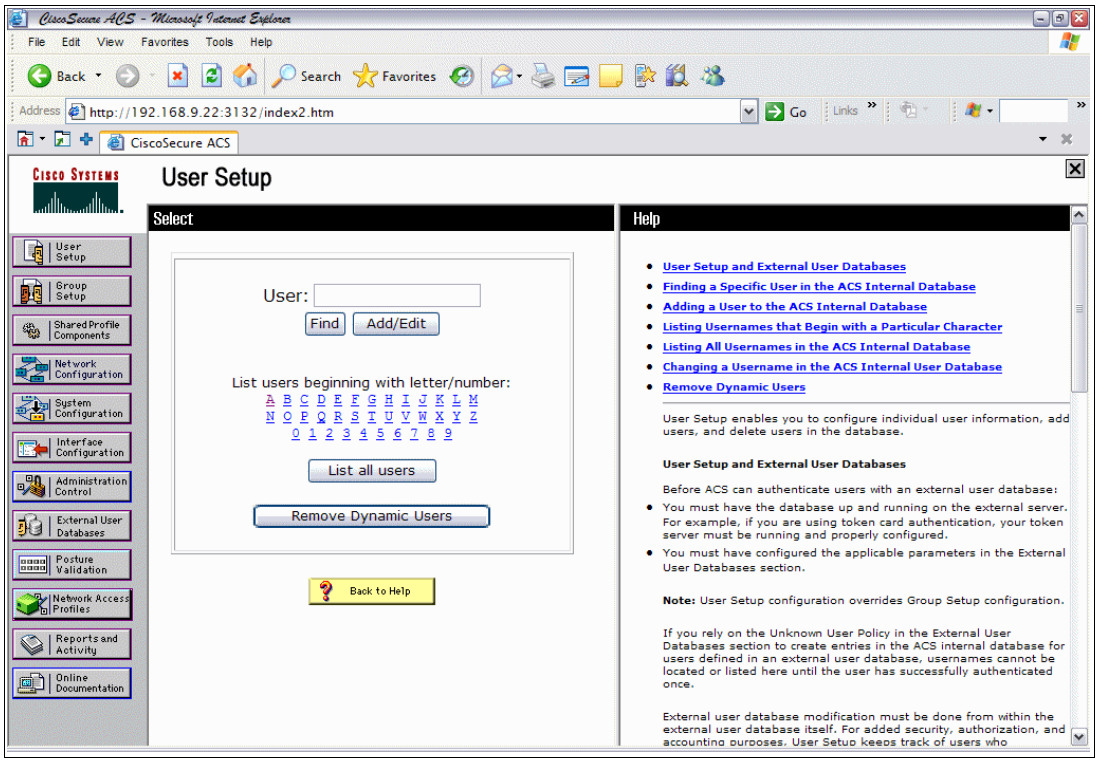

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3132/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Select
User:
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
User Setup enables you to configure individual user information, add users, and delete users in the database.
User Setup and External User Databases
Before ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.
External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who

Figure 7-22 User setup

2. In the User field, type the name of the user to be added, then click **Add/Edit**.

Downloaded from www.Manualslib.com manuals search engine

3. You will be prompted for the *user's real name* and *description* under Supplementary User Info, followed by *user setup details*, as shown in Figure 7-23. The password authentication, in this example, is set to *ACS Internal Database*, the password has been entered and confirmed, and the user has been assigned to a default group. The list of groups available will be a direct result of those you configured in Figure 7-21 on page 238.

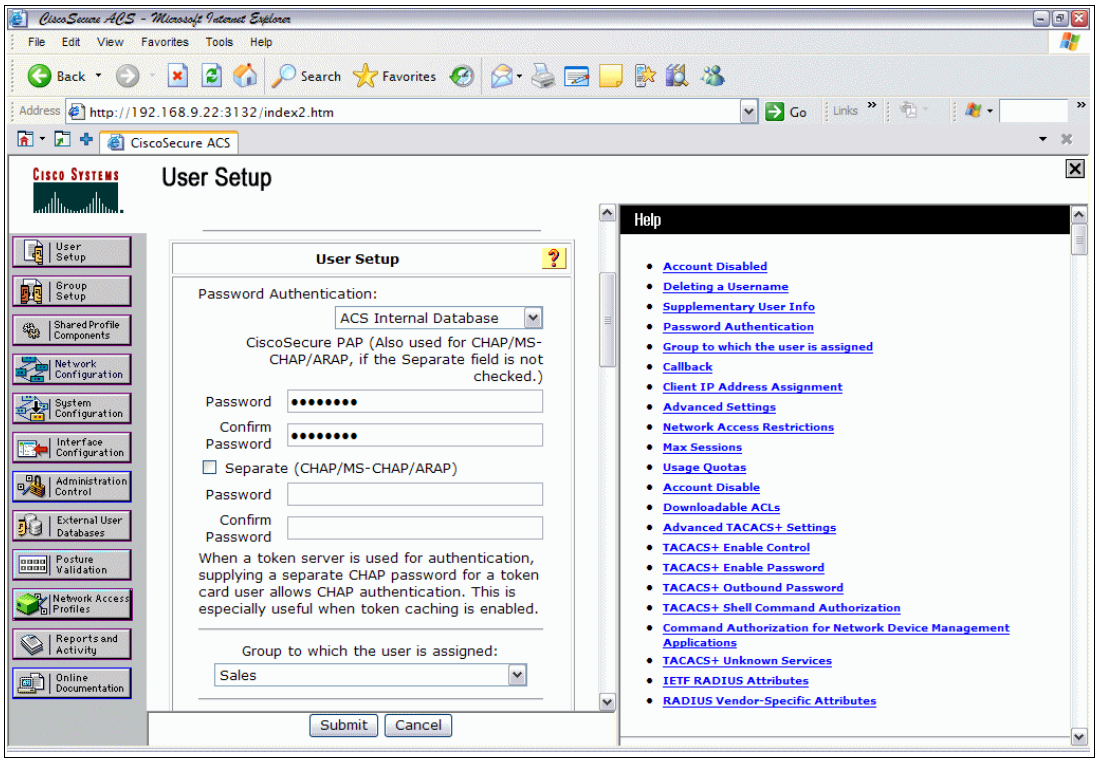


Figure 7-23 User-to-Group mappings

Downloaded from www.Manualslib.com manuals search engine

Global authentication setup

The Cisco Secure ACS supports many types of protocols for securely transferring credentials from the host to the Cisco Secure ACS for authentication and authorization.

Note: We highly recommend that you enable all protocols globally. You will have the opportunity to limit the actual protocol options later when you create the Network Access Profiles for NAC. If they are not enabled here, they will not be enabled in the Network Access Profiles.

1. Click **System Configuration** from the main menu and then select **Global Authentication Setup** (Figure 7-24).

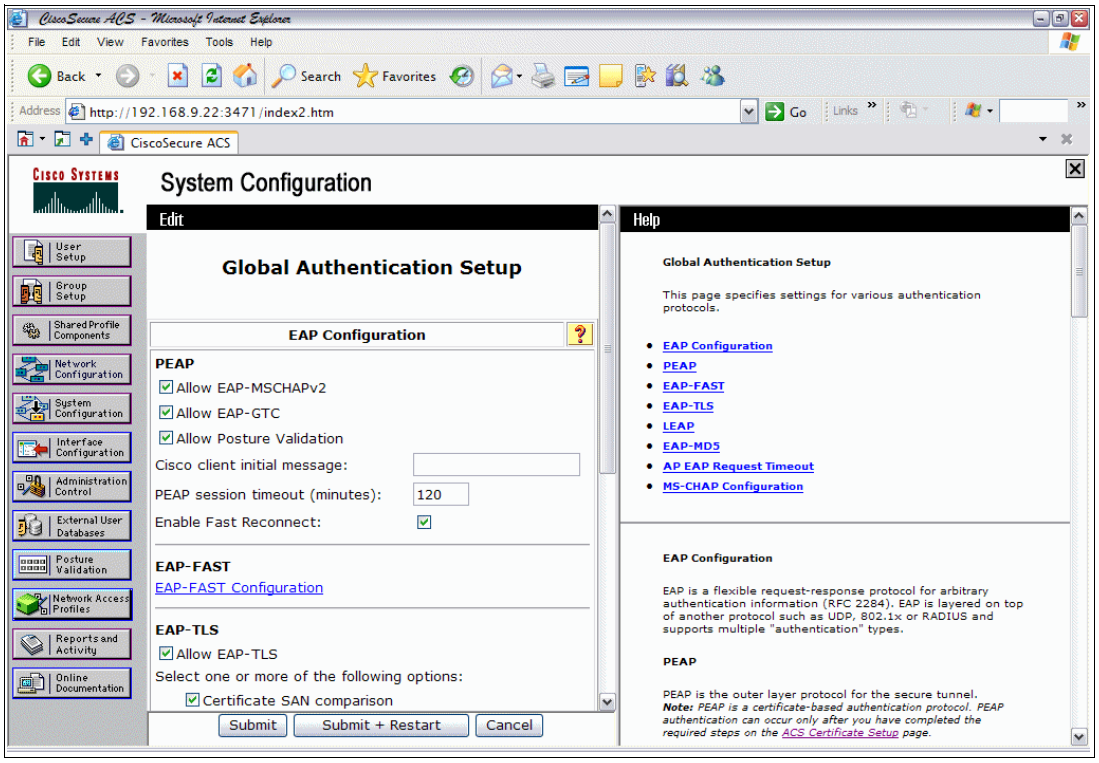


Figure 7-24 Global Authentication Setup

2. Make sure that each check box is selected, that Enable Fast Reconnect is selected, that PEAP and EAP-TLS time outs are set to 120 minutes.
3. Click **Submit + Restart**.

Downloaded from www.Manualslib.com manuals search engine

4. Click **EAP-FAST Configuration** from the Global Authentication Setup (Figure 7-24 on page 241).

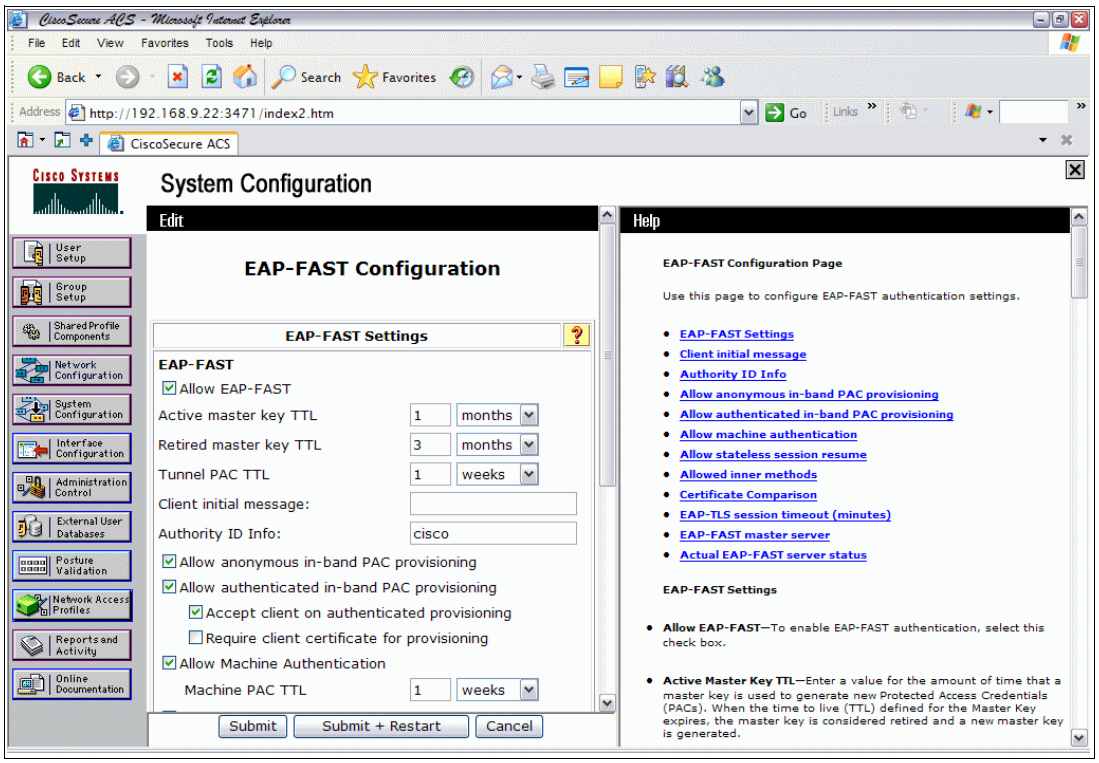

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3471/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
System Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
EAP-FAST Configuration
EAP-FAST Settings
EAP-FAST
Allow EAP-FAST
Active master key TTL 1 months
Retired master key TTL 3 months
Tunnel PAC TTL 1 weeks
Client initial message:
Authority ID Info: cisco
Allow anonymous in-band PAC provisioning
Allow authenticated in-band PAC provisioning
Accept client on authenticated provisioning
Require client certificate for provisioning
Allow Machine Authentication
Machine PAC TTL 1 weeks
Submit
Submit + Restart
Cancel
Help
EAP-FAST Configuration Page
Use this page to configure EAP-FAST authentication settings.
EAP-FAST Settings
Client initial message
Authority ID Info
Allow anonymous in-band PAC provisioning
Allow authenticated in-band PAC provisioning
Allow machine authentication
Allow stateless session resume
Allowed inner methods
Certificate Comparison
EAP-TLS session timeout (minutes)
EAP-FAST master server
Actual EAP-FAST server status
EAP-FAST Settings
Allow EAP-FAST—To enable EAP-FAST authentication, select this check box.
Active Master Key TTL—Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated.

Figure 7-25 EAP-FAST Configuration screen

5. The EAP-FAST configuration, as shown in Figure 7-25, requires you to enter a lot of fields. Table 7-1 lists all fields and their respective values.

Table 7-1 EAP-FAST Configuration values

EAP-FAST configuration	Condition
Allow EAP-FAST	Checked
Active Master Key TTL	One month
Retired Master Key TTL	Three months
Tunnel PAC TTL	One week
Client Initial Message	<nil>
Authority ID Info	cisco
Allow anonymous in-band PAC provisioning	Checked
Accept client on authenticated provisioning	Checked

Downloaded from www.Manualslib.com manuals search engine

EAP-FAST configuration	Condition
Require client certificate for provisioning	Checked
Allow Machine Authentication	Checked
Machine PAC TTL	One week
Allow Stateless Session Resume	Checked
Authorization PAC TTL	One hour
Allow inner methods	
EAP-GTC	Checked
EAP-MSCHAPv2	Checked
EAP-TLS	Checked
Select one or more of the following EAP-TLS comparison methods:	
Certificate SAN comparison	Checked
Certificate CN comparison	Checked
Certificate Binary comparison	Checked
EAP-TLS Session timeout (minutes)	120
EAP-FAST Master Server	Checked
Actual EAP-FAST Server status	Master

6. Click **Submit + Restart**.

Downloaded from www.Manualslib.com manuals search engine

Configuring posture validation

To do this:

1. Select **Posture Validation** from the Main Menu (Figure 7-26).

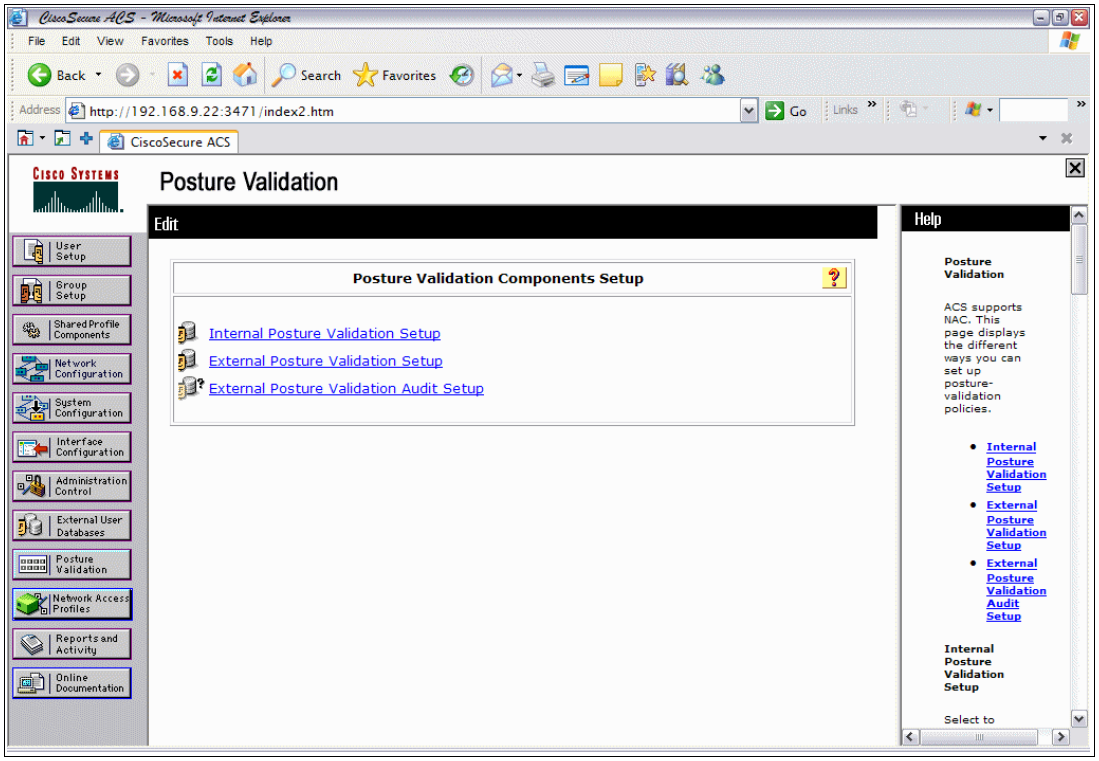


Figure 7-26 Posture Validation

Downloaded from www.Manualslib.com manuals search engine

2. Select **Internal Posture Validation**. The screen show in Figure 7-27 will be displayed.
3. Click **Add Policy** (Figure 7-27).

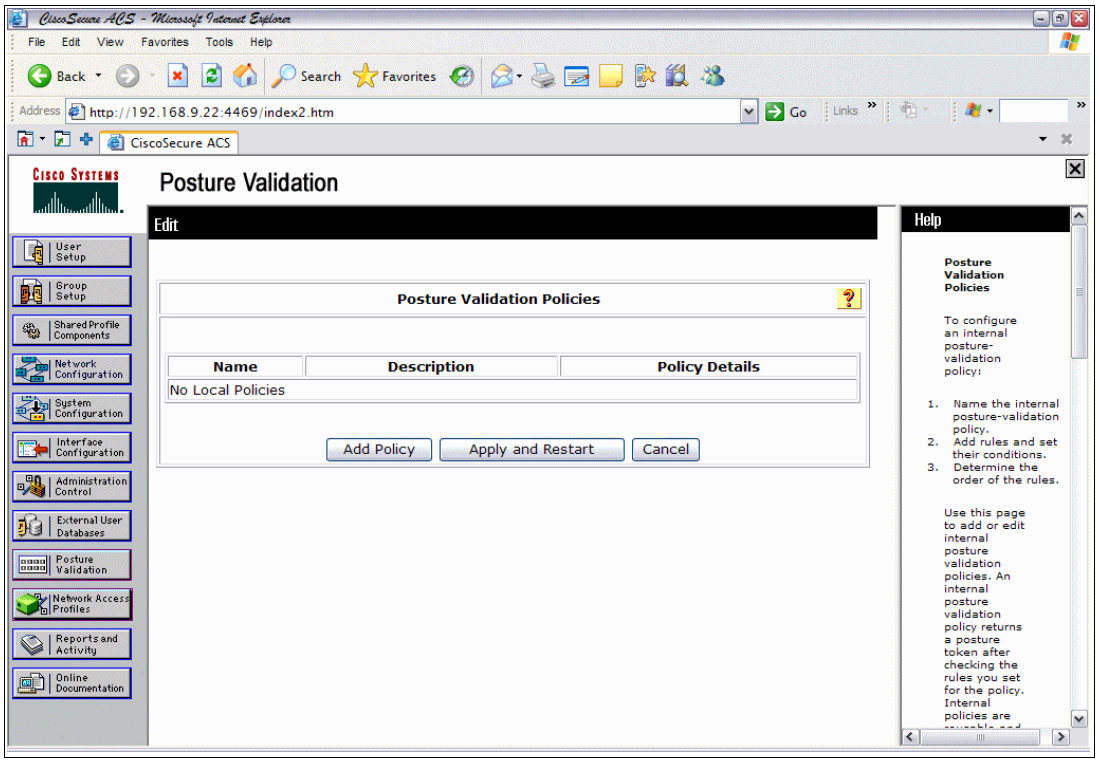


Figure 7-27 Posture Validation Policies

Downloaded from www.Manualslib.com manuals search engine

4. In this example, we have entered the name of the first policy as CTA with the description Cisco Trust Agent. Then click **Submit** (Figure 7-28).

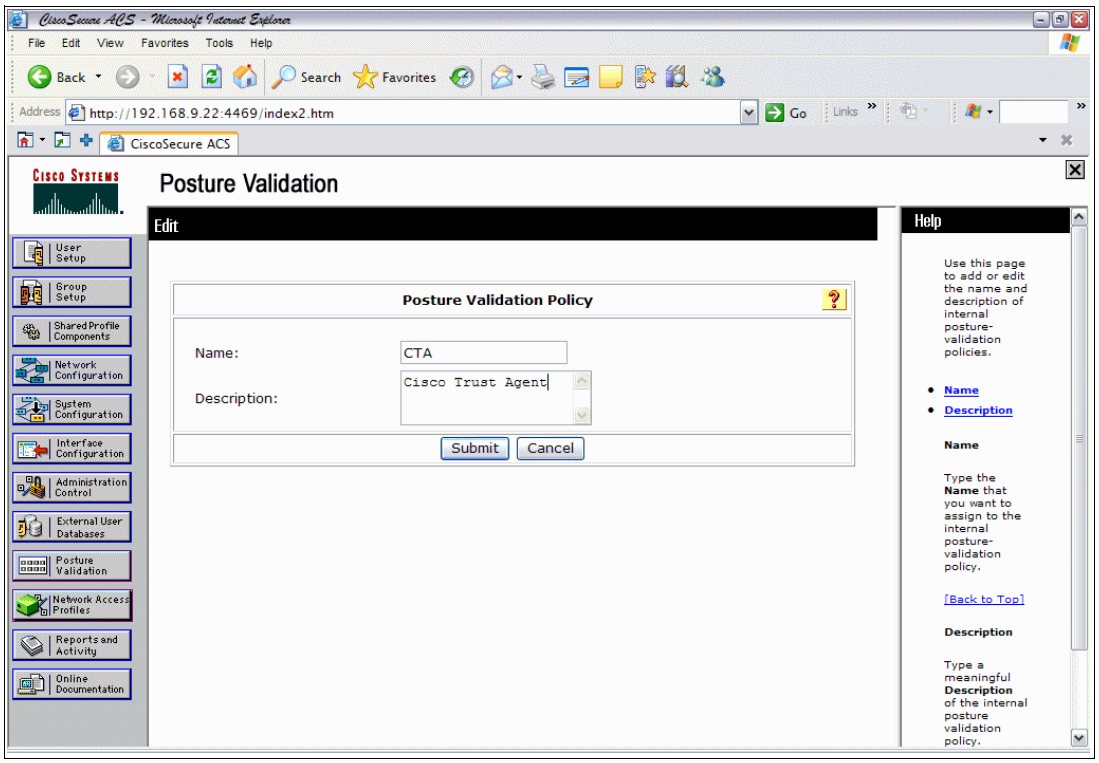


Figure 7-28 CTA Posture Validation Policy

Downloaded from www.Manualslib.com manuals search engine

5. Click **Add Rule** (Figure 7-29).

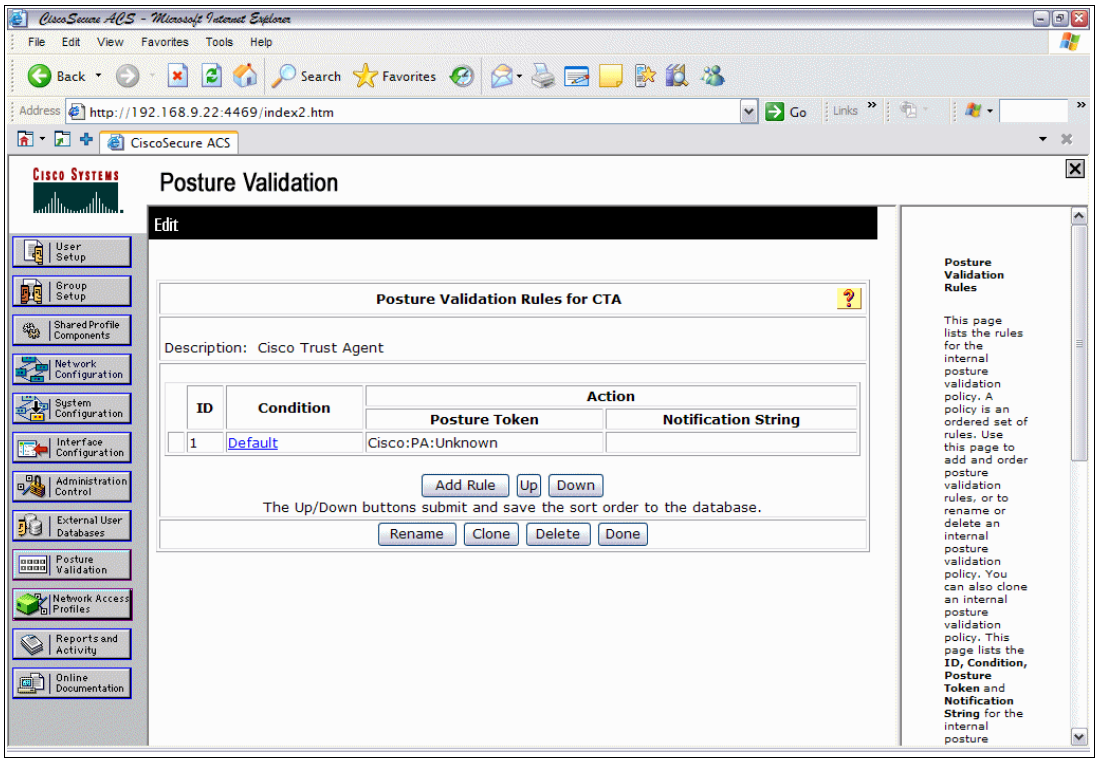


Figure 7-29 Posture Validation for CTA

Downloaded from www.Manualslib.com manuals search engine

6. Click **Add Condition Set** (Figure 7-30).

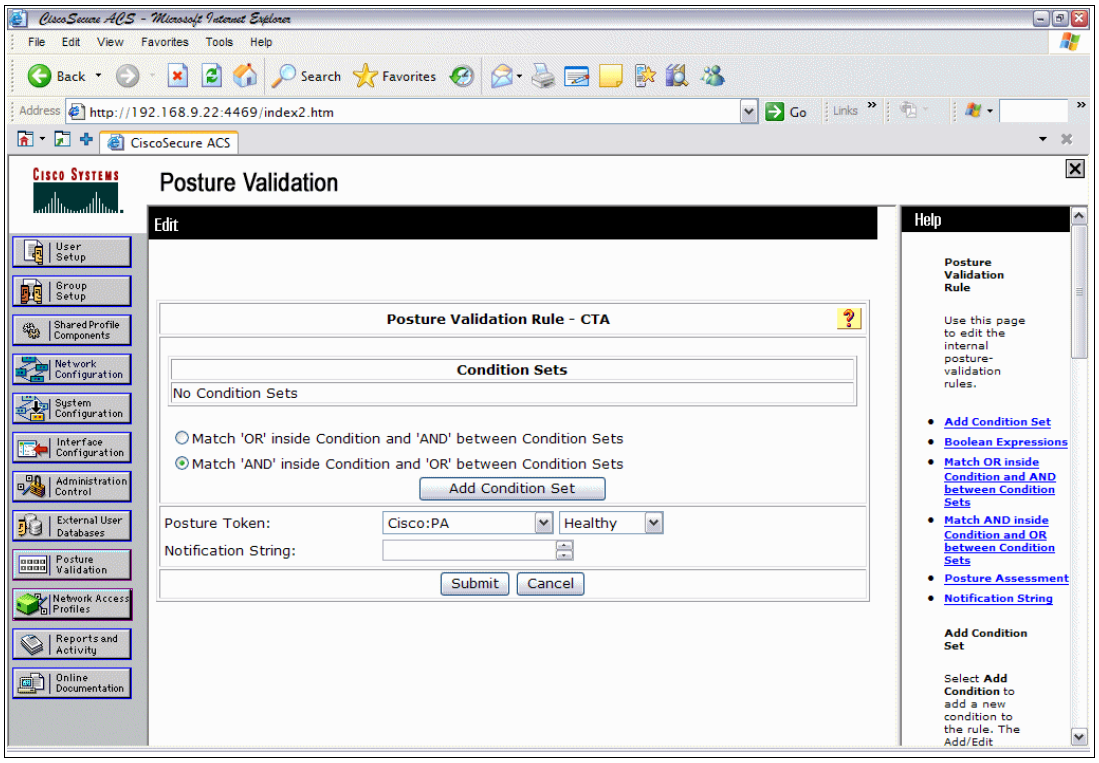


Figure 7-30 Condition sets for CTA policy

Downloaded from www.Manualslib.com manuals search engine

7. From the Attribute drop-down list (Figure 7-31), select **Cisco:PA:PA-Version**. The operator value should be set to >= and the value set to 2.0.0.0. This simply means that we are setting up a check for the Cisco Trust Agent to be present on the endpoint, and that it must be running version 2.0.0.0 or later. Click **Enter** when this is done, and then **Submit**.

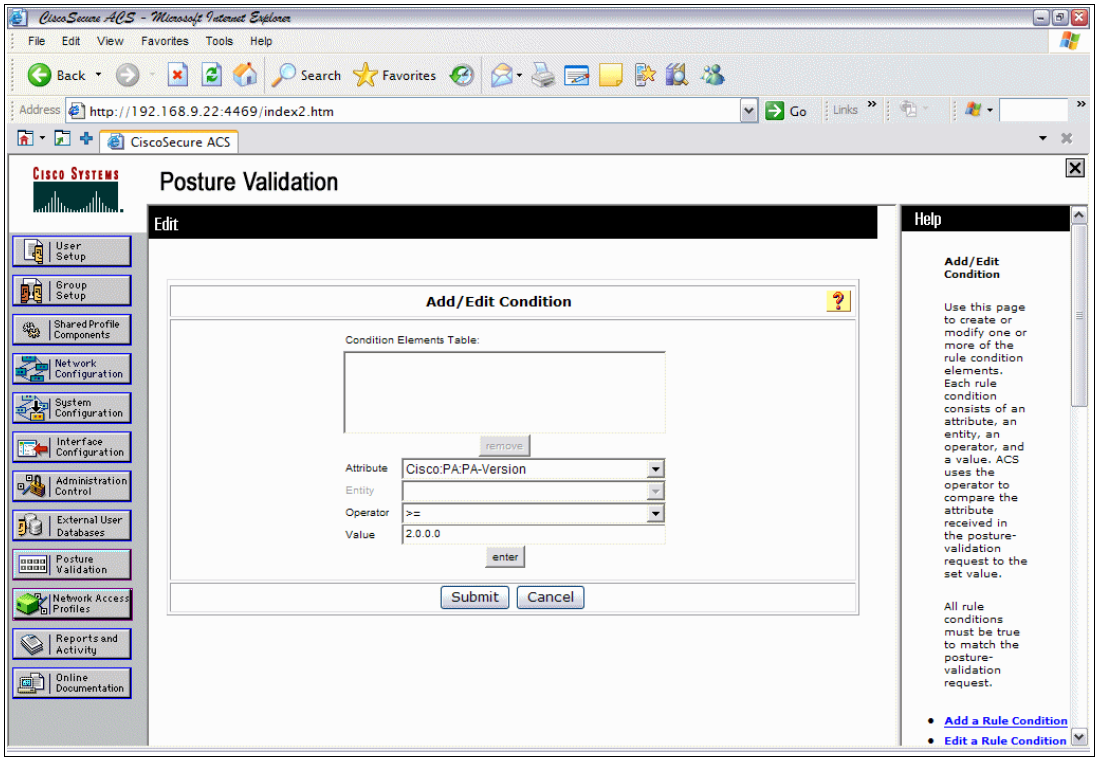


Figure 7-31 Adding a condition set

Downloaded from www.Manualslib.com manuals search engine

8. Figure 7-32 shows that if this condition is satisfied, that an Application Posture Token (APT) of *Healthy* is returned. Clicking **Submit** here takes us to Figure 7-33 on page 251.

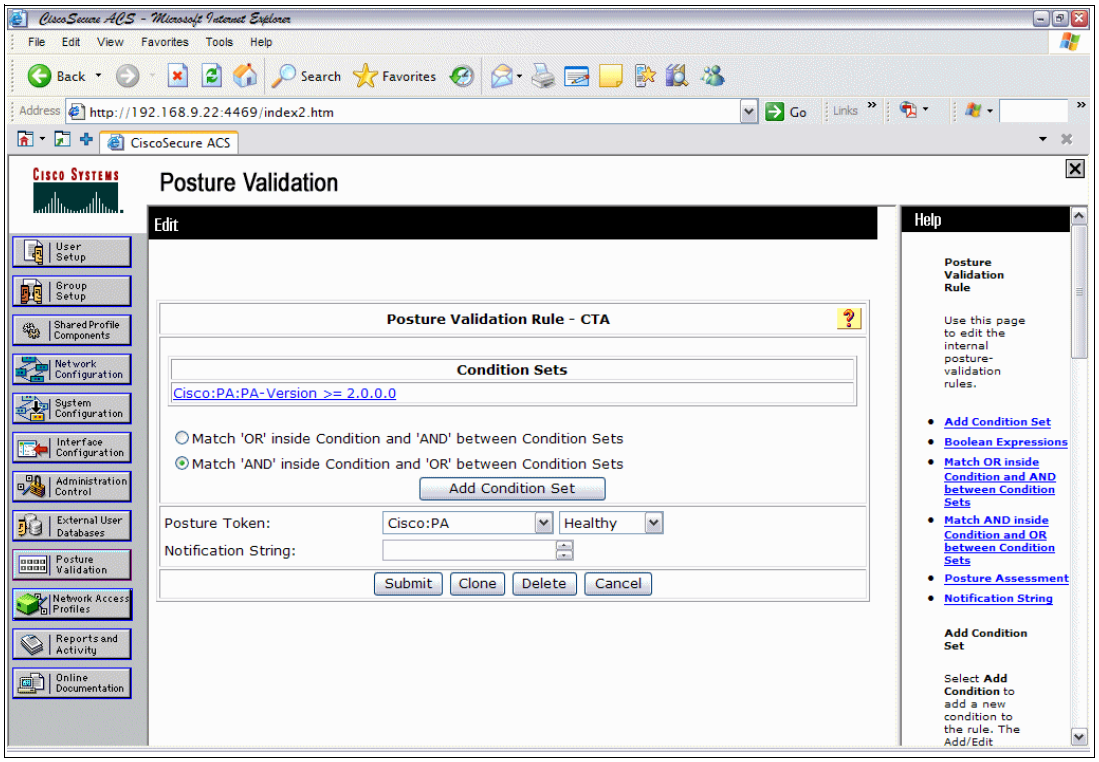


Figure 7-32 Posture validation rule creation for CTA check

Downloaded from www.Manualslib.com manuals search engine

9. Next we need to modify the default action, which is the action to be taken if the condition we just created is not met. You will notice that there is a default condition, which we will modify for this purpose. Click **Default** under Condition (Figure 7-33).

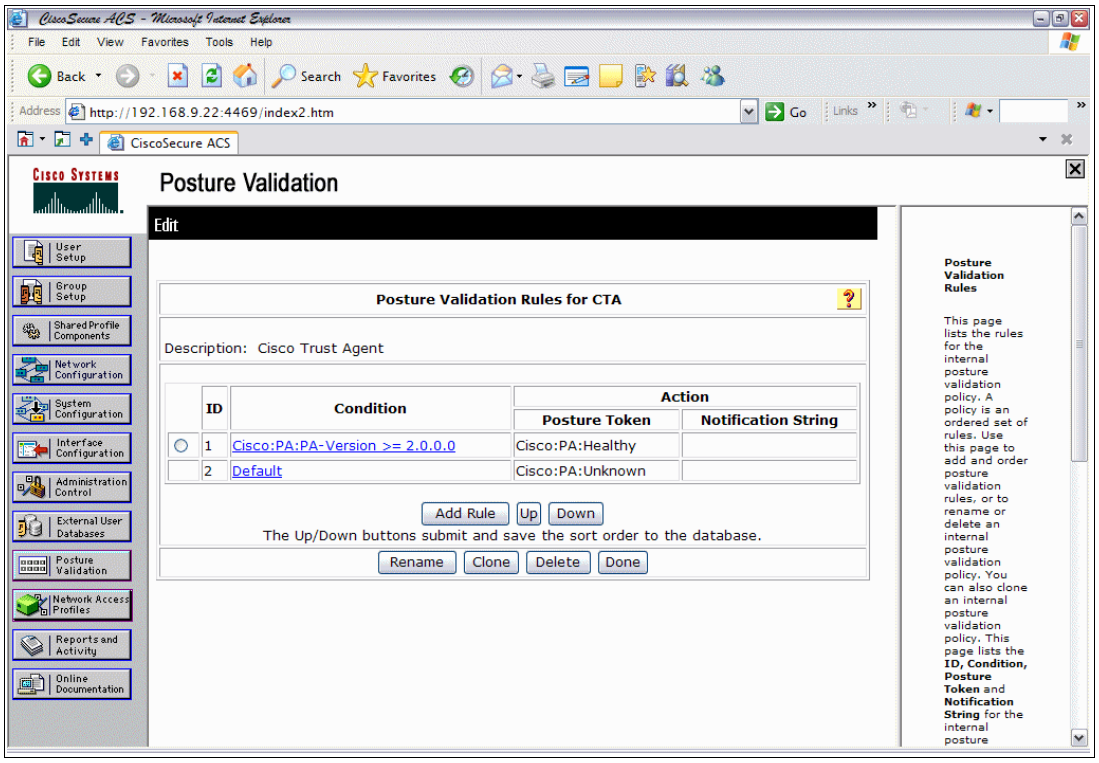


Figure 7-33 CTA rule defined

Downloaded from www.Manualslib.com manuals search engine

10. The posture token remains Cisco:PA, however the posture token value should be changed to *Quarantine*, as shown in Figure 7-34. In the notification string, add the line:

```
http://tcmweb/SoftwarePackageServerWeb/SPServlet
```

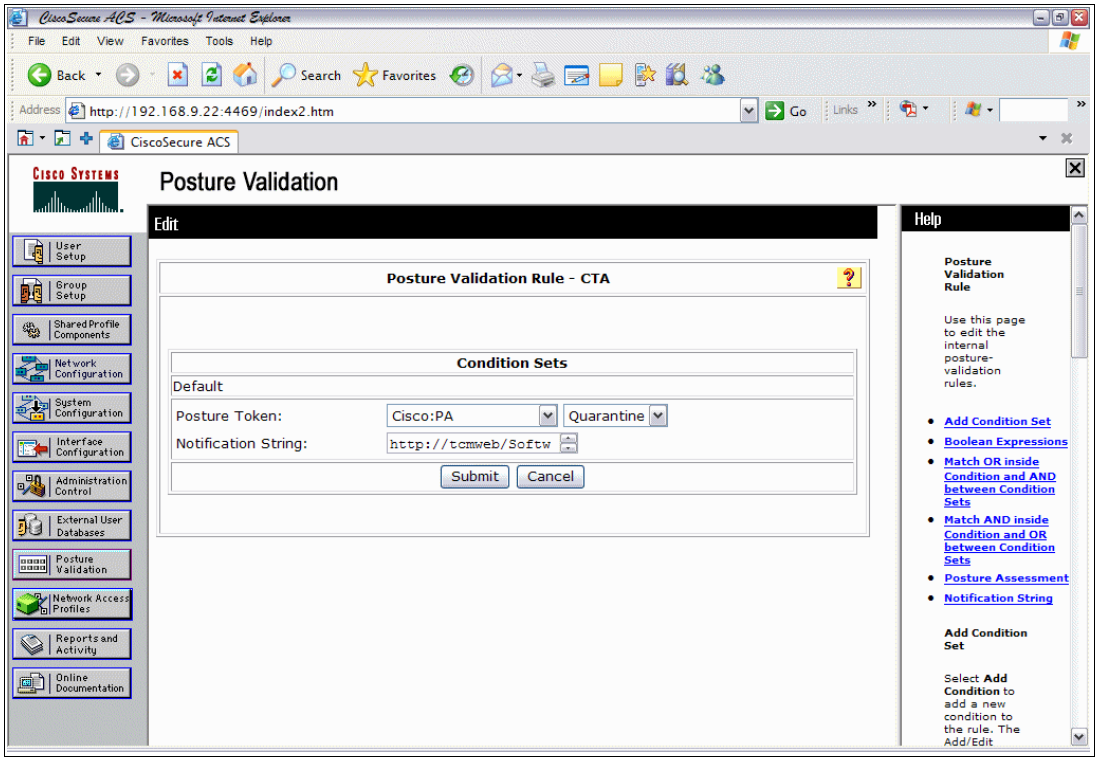


Figure 7-34 Quarantine condition applied as default action

Note: http://tcmweb/SoftwarePackageServerWeb/SPServlet is the location of the software remediation package. The URL can be changed depending on where the remediation software packages are stored.

Downloaded from www.Manualslib.com manuals search engine

11. Click **Submit** and you will find yourself back in the dialog shown in Figure 7-35.

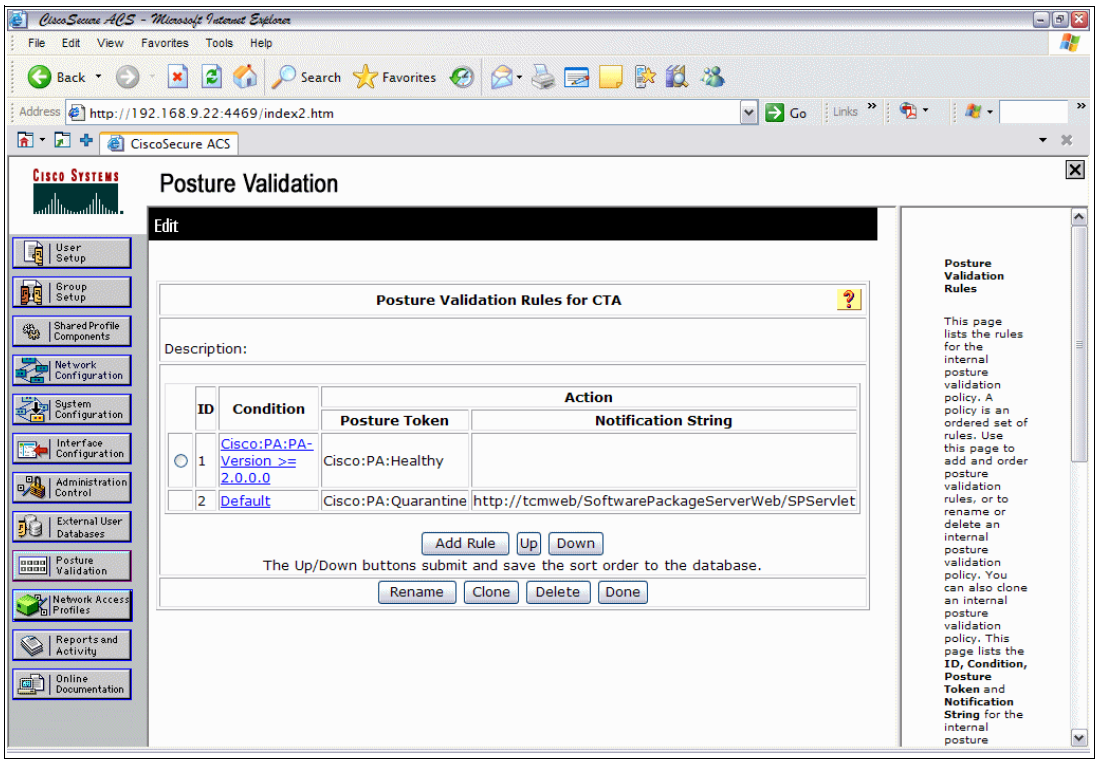


Figure 7-35 Completed posture validation for CTA

12. Click **Done**.

Downloaded from www.Manualslib.com manuals search engine

13. Click **Apply and Restart**, as shown in Figure 7-36.

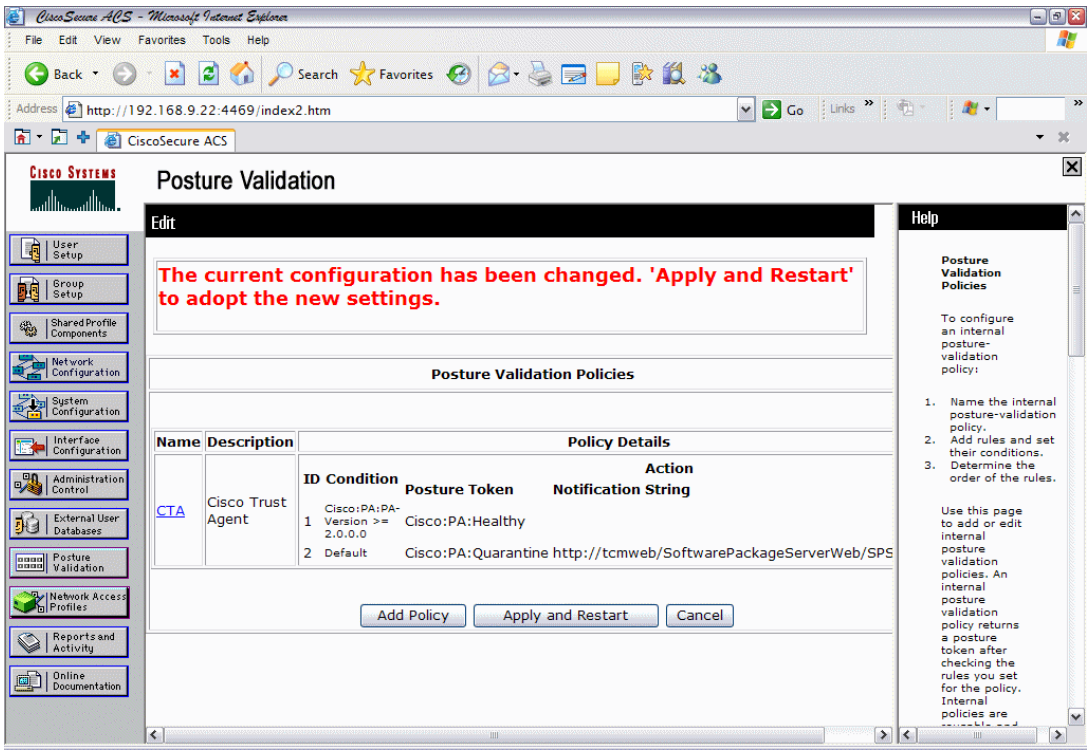


Figure 7-36 CTA posture validation policy

14. Next we must repeat the process to create a posture check for the IBM:SCM.

Downloaded from www.Manualslib.com manuals search engine

15. Click **Add Policy** (Figure 7-37).

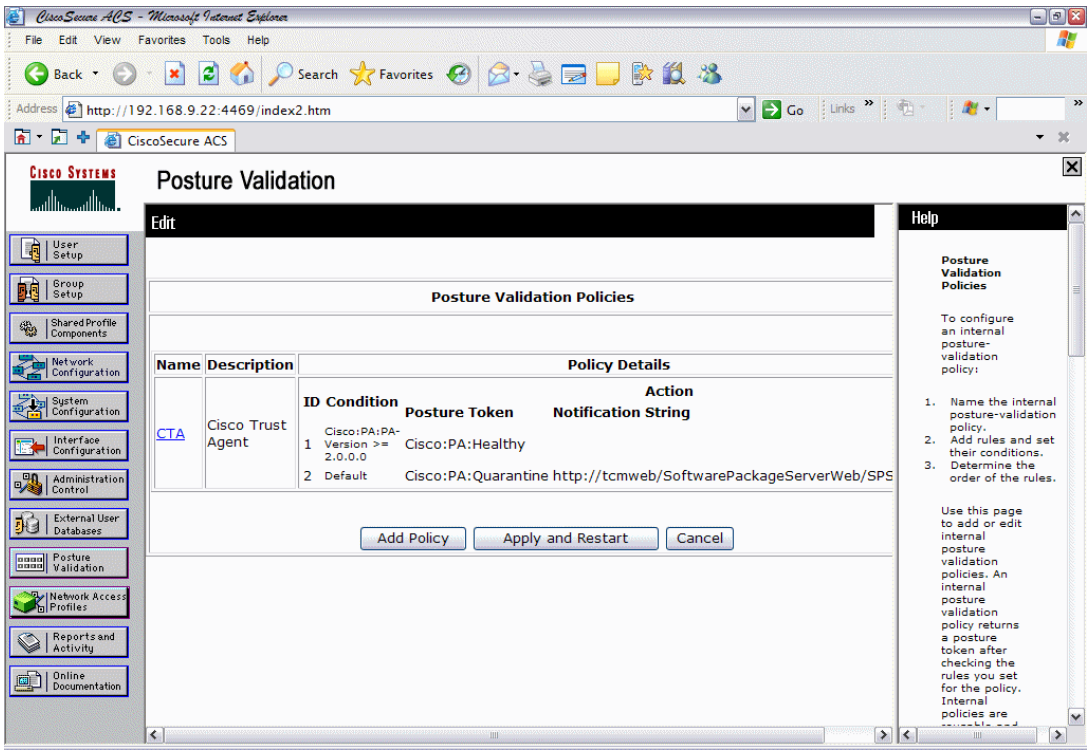


Figure 7-37 Repeating the process for Security Compliance Manager

Downloaded from www.Manualslib.com manuals search engine

16. In this example, we use TSCM in the Name field and IBM Security Compliance in the Description field, as shown in Figure 7-38.

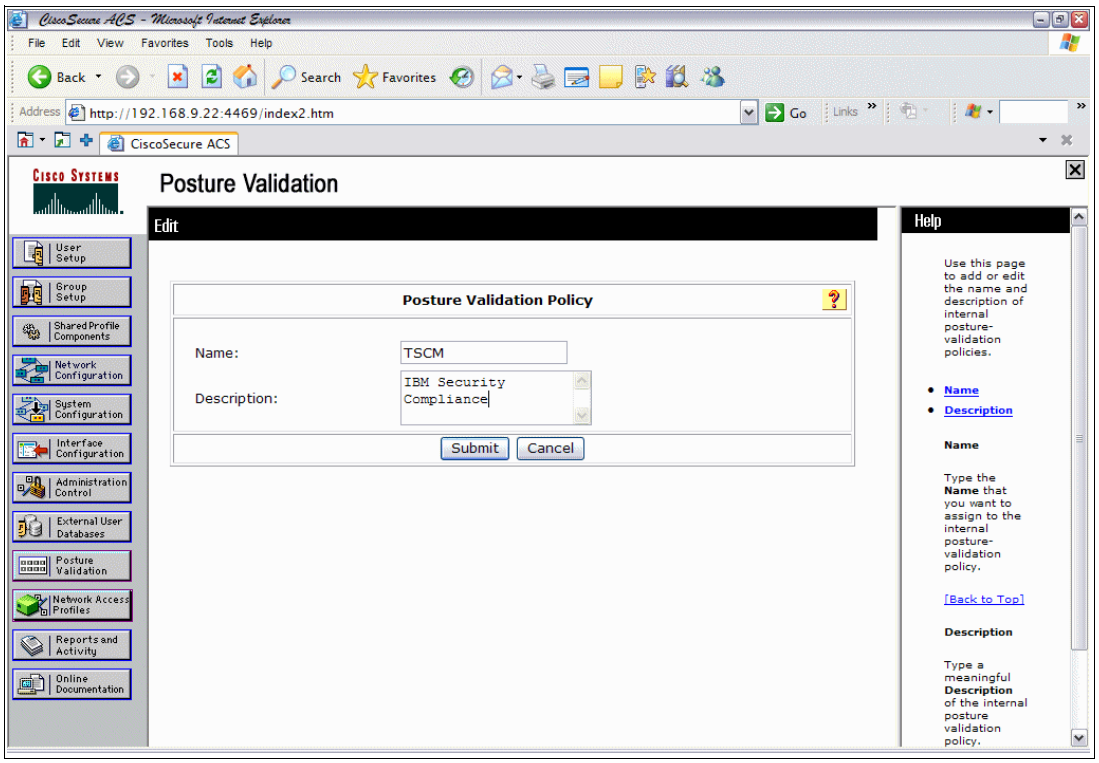


Figure 7-38 IBM TSCM policy creation

Downloaded from www.Manualslib.com manuals search engine

17. After entering the name and description, click **Submit** and you will see the dialog shown in Figure 7-39.

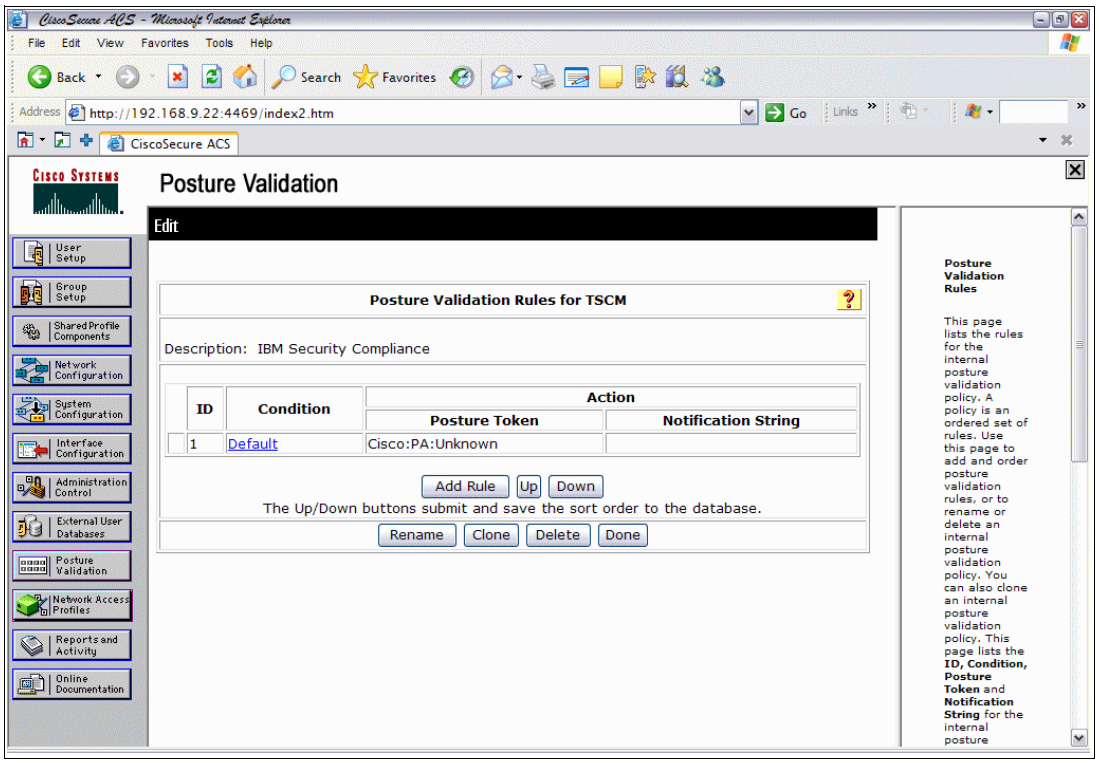


Figure 7-39 IBM TSCM policy creation

Downloaded from www.Manualslib.com manuals search engine

18. Click **Add Rule** to get to the screen shown in Figure 7-40.

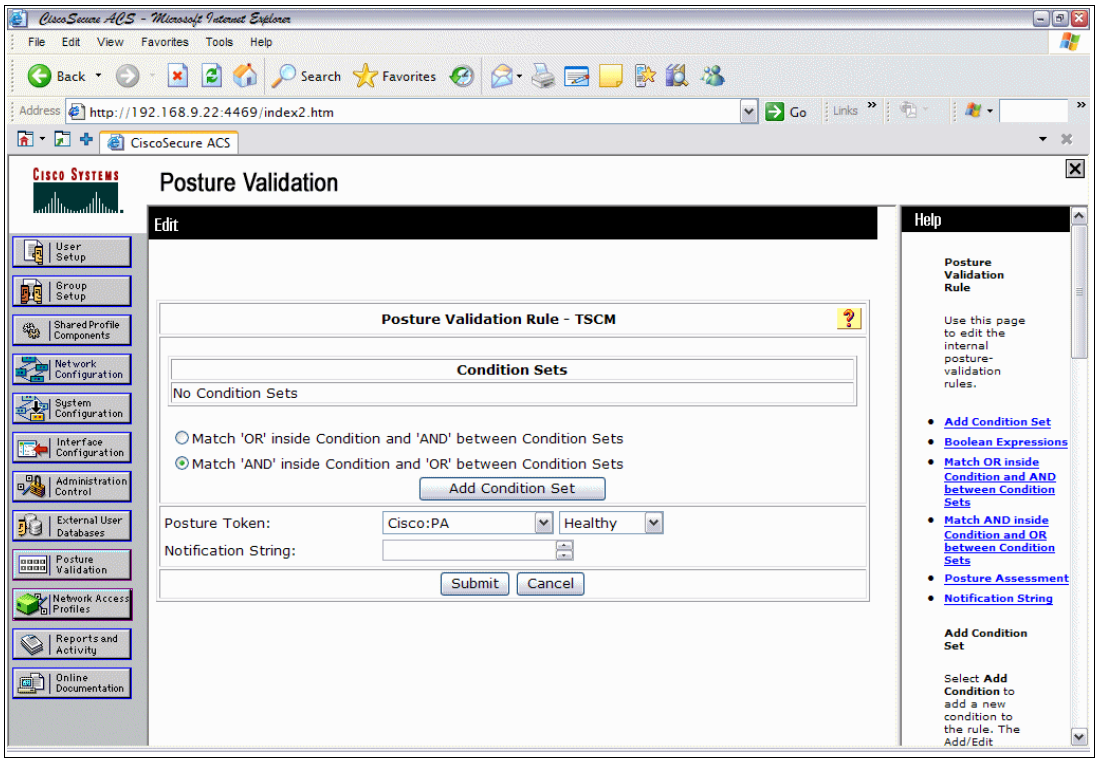


Figure 7-40 Condition set creation for TSCM

19. Click **Add Condition Set**. From the Attribute drop-down menu, select **IBMCorporation:SCM:PolicyVersion**. From the Operator menu select **Contains**, and for the Value enter the value of the security policy being used on the Security Compliance Manager server. In this example, the policy version is IISSCN_EBU_v2.20_winXP. Click **Enter**.

> **Note:** This is to enforce the version of the TSCM policy being used. There is only an exact match option available. This means that all clients will be running the same policy version. It is critical when setting this check that you get the policy version name and syntax correct or the checks will fail. We also discovered that if you set the operator value to an equals sign (=), the check will fail even though the end user is running the correct version of the policy.

Downloaded from www.Manualslib.com manuals search engine

20. From the Attribute drop-down menu, select **IBMCorporation:SCM:PolicyViolation.** From the Operator menu select =, and for the Value enter 0. Then click **Enter** (Figure 7-41).

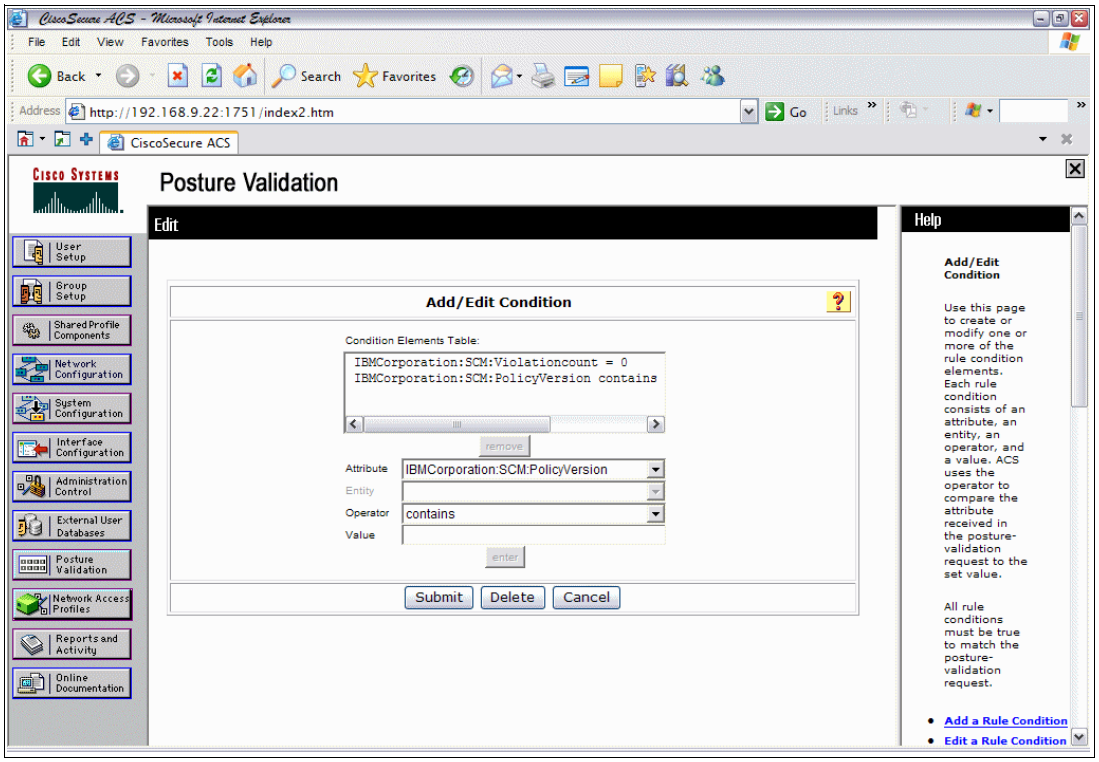


Figure 7-41 TSCM policy components

21. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

22. Make sure that the posture token is set to IBMCorporation:SCM, and the value should be set to Healthy (Figure 7-42).

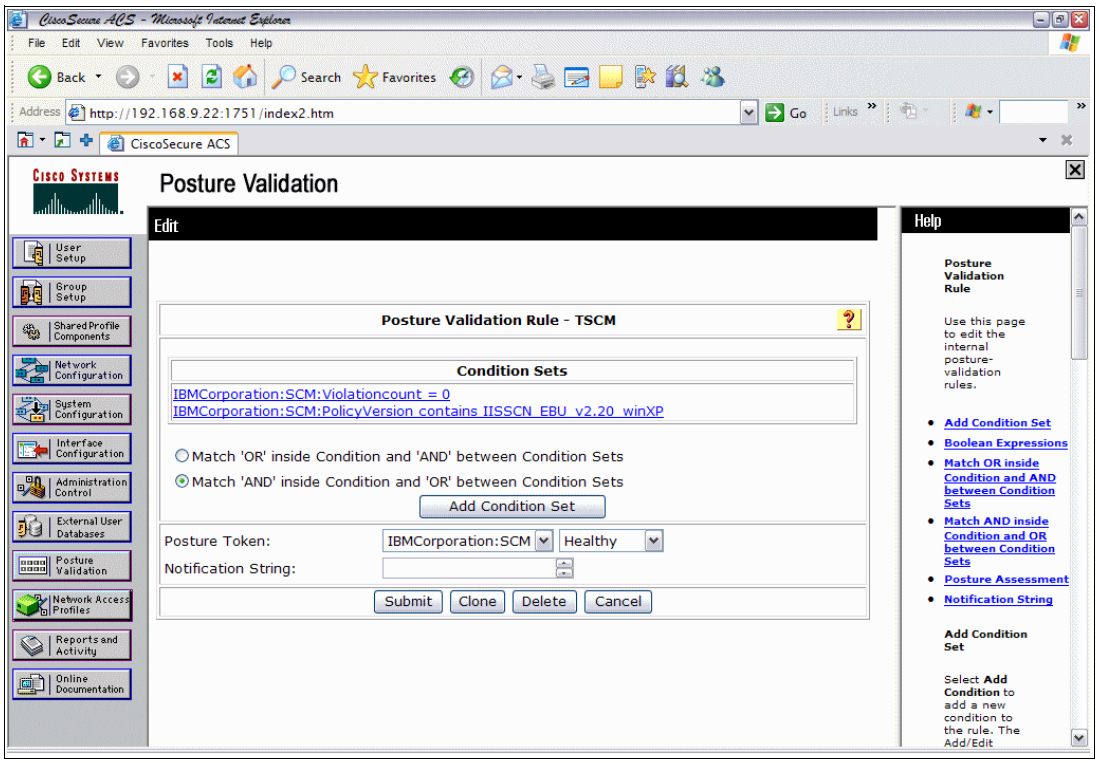


Figure 7-42 Completed posture validation check for Security Compliance Manager

23. Click **Submit**.

24. Next we must modify the default condition. Click **Default,** as shown in Figure 7-39 on page 257.

Downloaded from www.Manualslib.com manuals search engine

25. The posture token should be set to *IBMCorporation:SCM* (Figure 7-43) and the value should be set to *Quarantine*. The notification string should be the same as we discussed in step 10 on page 252 of this section:

```
http://tcmweb/SoftwarePackageServerWeb/SPServlet
```

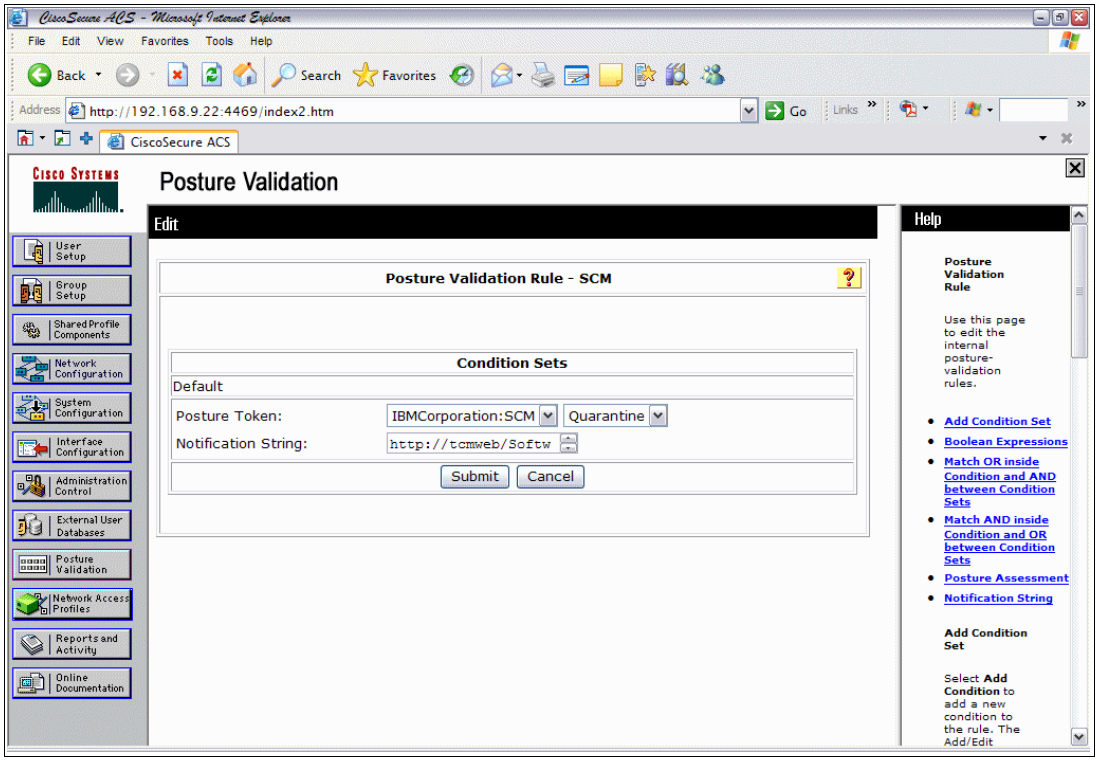


Figure 7-43 Security Compliance Manager Default condition modification

26. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

27. Click **Done** (Figure 7-44).

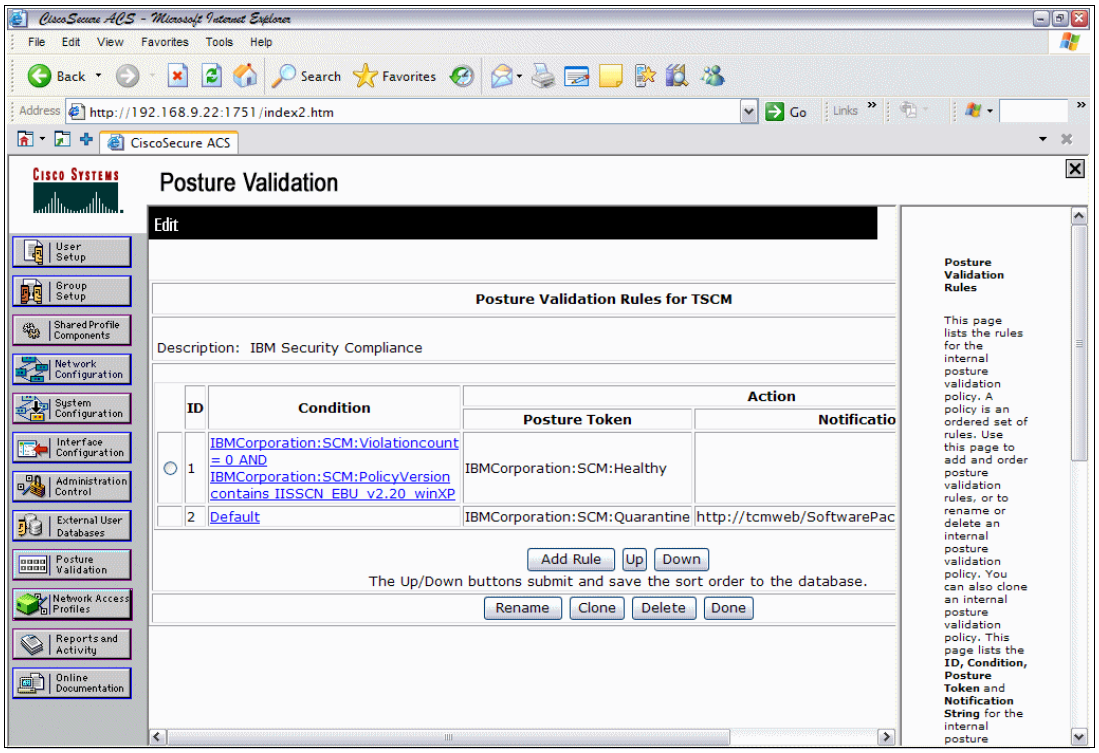


Figure 7-44 Completed Security Compliance Manager posture validation

Downloaded from www.Manualslib.com manuals search engine

28. Click **Apply and Restart** (Figure 7-45).

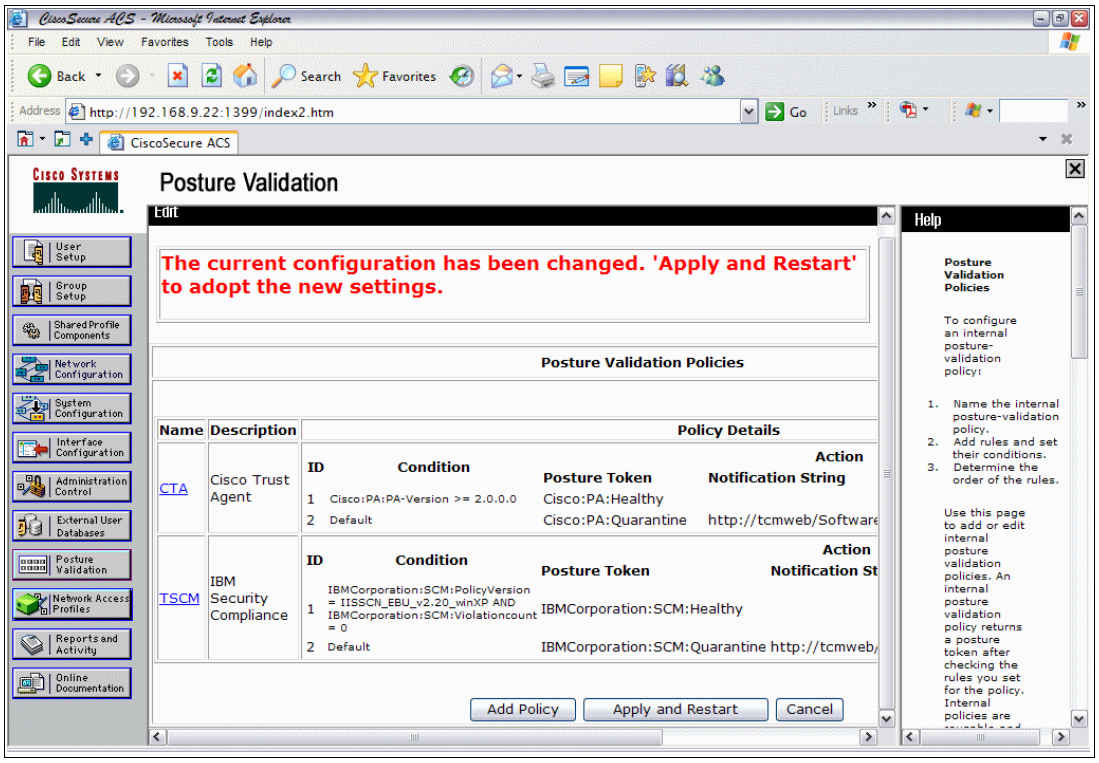


Figure 7-45 Completed posture validation rules

Downloaded from www.Manualslib.com manuals search engine

Configuring RADIUS Authorization Components

In this section we configure RADIUS Authorization Components (RAs), a new concept introduced with Cisco Secure ACS 4.0.

Note: We deleted all of the default RACs and started with a blank screen. It was cleaner to work with and take you through the steps of creating a RAC from scratch, as opposed to cloning an existing example.

1. Click **Shared Profile Components** from the main menu. This brings you to the dialog shown in Figure 7-46.

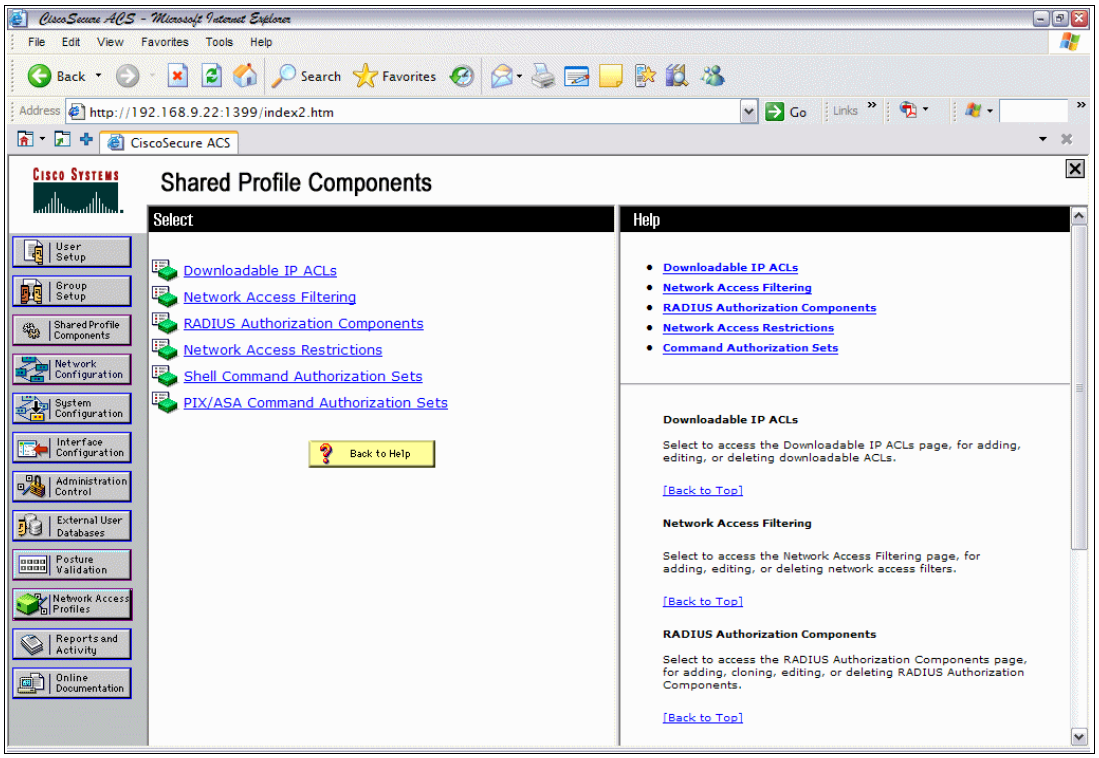


Figure 7-46 Shared Profile Components

2. Click **RADIUS Authorization Components**.

Downloaded from www.Manualslib.com manuals search engine

Note: In the scenario detailed in this book, we have two groups defined: sales and engineering. When creating the RACs, we define a Healthy Sales RAC, a Quarantine Sales RAC, a Healthy Engineering RAC, and a Quarantine engineering RAC. We also define a Default Quarantine RAC to address the situation where a condition may not be defined or there is no matched condition. When a user authenticates via IEEE 802.1x, the posture is checked and a RAC is applied. In this way, we can have individual Quarantine VLANs for the different groups, which also allows for different access restrictions for different Quarantine groups. This was done to show how the solution scales. Have a clear plan on your group to VLAN mappings, and your VLAN structure before configuring this portion. We used the following:

- Healthy Sales - VLAN 11
- Healthy Engineering - VLAN 12
- Quarantine Sales - VLAN 13
- Quarantine Engineering - VLAN 14
- Default Quarantine - VLAN 15

3. Click **Add**.
4. To create the Healthy Sales RAC, in the Name field type `Healthy_Sales_RAC`.
5. In the Add New Attribute section, we are using the drop-down menus to add the required values, which are described in Table 7-2.

Table 7-2 Healthy Sales RAC attributes

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=healthy_hosts
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)
IETF	Tunnel-Type (64)	[T1] VLAN (13)
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
IETF	Tunnel-Private-Group-ID (81)	[T1] 11

Downloaded from www.Manualslib.com manuals search engine

6. Click **Add** next to Cisco IOS/PIX6.0, which brings you to Figure 7-47.

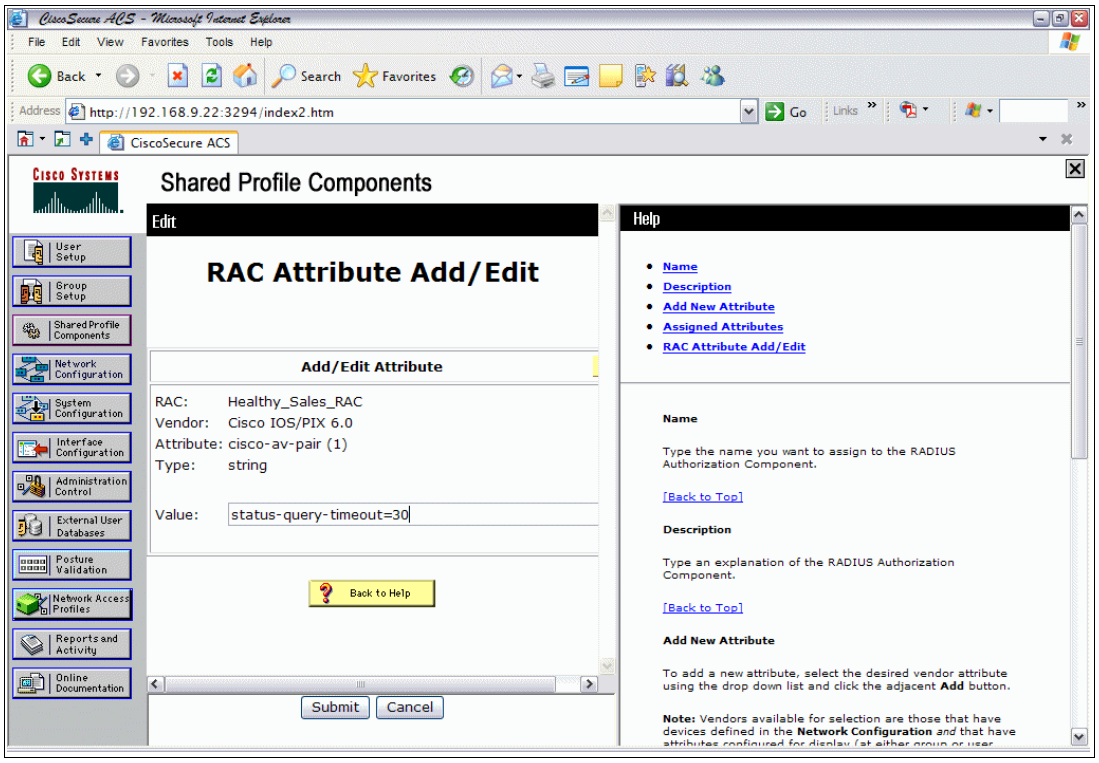


Figure 7-47 IOS RAC attribute

7. In the value field, enter `status-query-timeout=30`.
8. Click **Submit**.
9. Repeat this procedure, clicking **Add** next to Cisco IOS/PIX 6.0 and add the values as per Table 7-2 on page 265 for the Cisco IOS/PIX 6.0 requirements.

Downloaded from www.Manualslib.com manuals search engine

10. Repeat the same procedure for the IETF attributes, first selecting the relevant field from the drop-down menu, then clicking **Add** (Figure 7-48). Use the values in Table 7-2 on page 265.

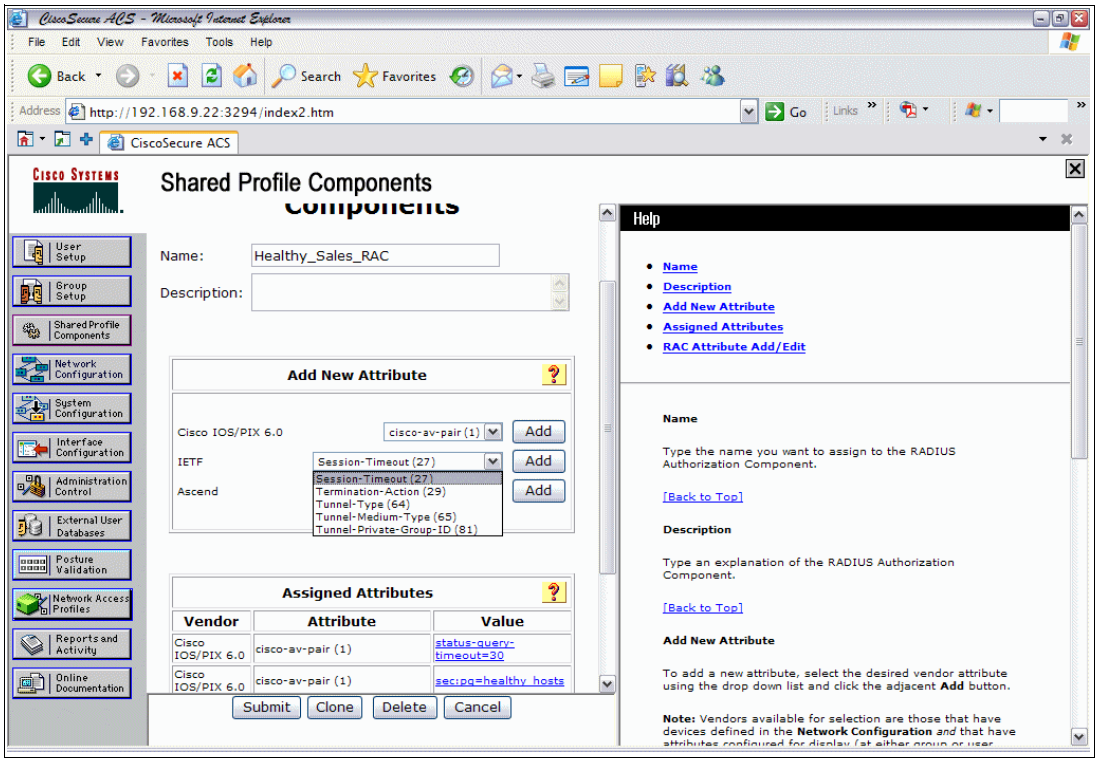


Figure 7-48 IETF drop-down menu

Downloaded from www.Manualslib.com manuals search engine

11. When completed, your Healthy Sales RAC should look like Figure 7-49.

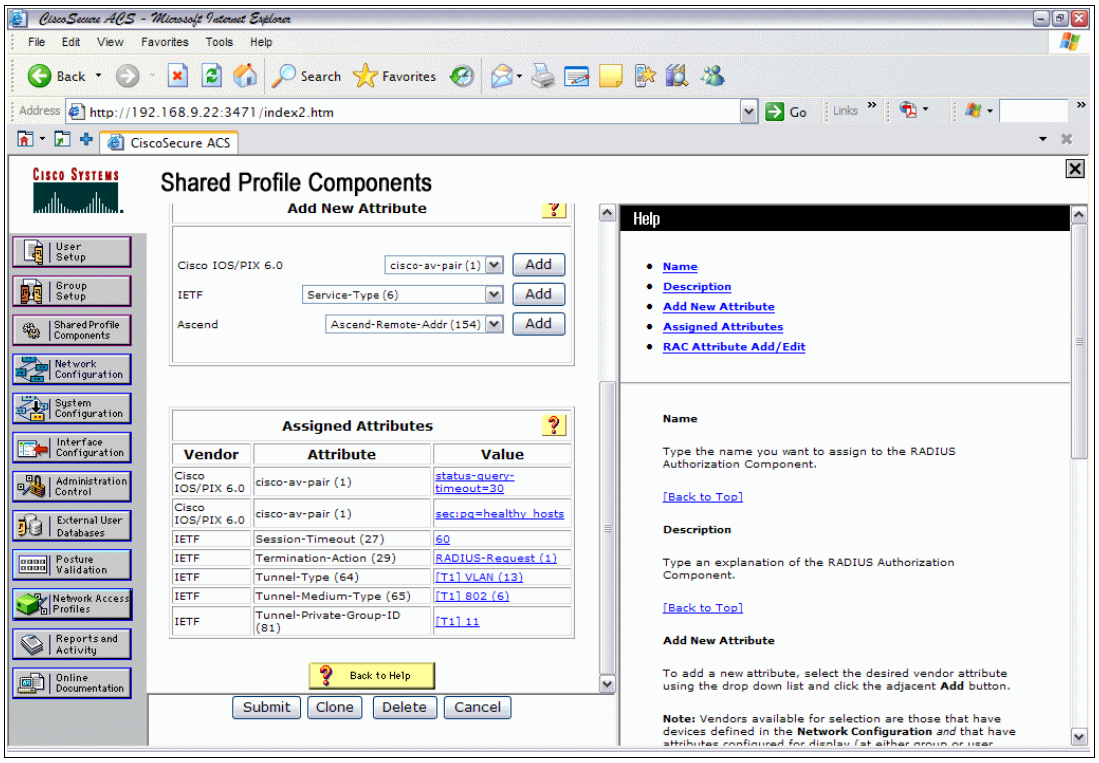


Figure 7-49 Healthy Sales RAC

12. Click **Submit**.

13. Repeat steps 3 through to 12 for each of the RACs to be configured. Using our example, there are the Healthy Engineering RAC, the Quarantine Sales RAC, the Quarantine Engineering RAC, and the Default Quarantine RAC to be configured. The values for each can be found in the following tables.

Table 7-3 Healthy Engineering RAC attributes

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=healthy_hosts
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)
IETF	Tunnel-Type (64)	[T1] VLAN (13)
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)

Downloaded from www.Manualslib.com manuals search engine

Vendor	Attribute	Value
IETF	Tunnel-Private-Group-ID (81)	[T1] 12

Table 7-4 Quarantine Sales RAC attributes

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=quarantine_hosts
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)
IETF	Tunnel-Type (64)	[T1] VLAN (13)
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
IETF	Tunnel-Private-Group-ID (81)	[T1] 13

Table 7-5 Quarantine Engineering RAC attributes

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=quarantine_hosts
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)
IETF	Tunnel-Type (64)	[T1] VLAN (13)
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
IETF	Tunnel-Private-Group-ID (81)	[T1] 14

Table 7-6 Default Quarantine RAC attributes

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=quarantine_hosts
IETF	Session-Timeout (27)	3600

Downloaded from www.Manualslib.com manuals search engine

Vendor	Attribute	Value
IETF	Termination-Action (29)	RADIUS-Request(1)
IETF	Tunnel-Type (64)	[T1] VLAN (13)
IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
IETF	Tunnel-Private-Group-ID (81)	[T1] 15

Note: The dot1x reauthentication timer is controlled by the value assigned to the IETF Session-Timeout (27) attribute. If set to 60, for example, the CTA pop-up screen will appear on the client workstation every 60 seconds. There will be some fine tuning required to find an appropriate value here. Entering the command **`show dot1x interface fa1/0/x detail`** shows that the reauthentication timers are *from auth server* — in other words, this field is from the ACS.

Downloaded from www.Manualslib.com manuals search engine

Configuring Network Access Profiles

We have now configured all of the individual components to be in a position to bring them together and create the Network Access Profiles, which determine what to check and what action to take based on the results of those checks. Again, we have deleted all of the pre-configured sample configs to create our own from scratch.

1. Select **Network Access Profiles** from the main menu, which brings you to the dialog in Figure 7-50.

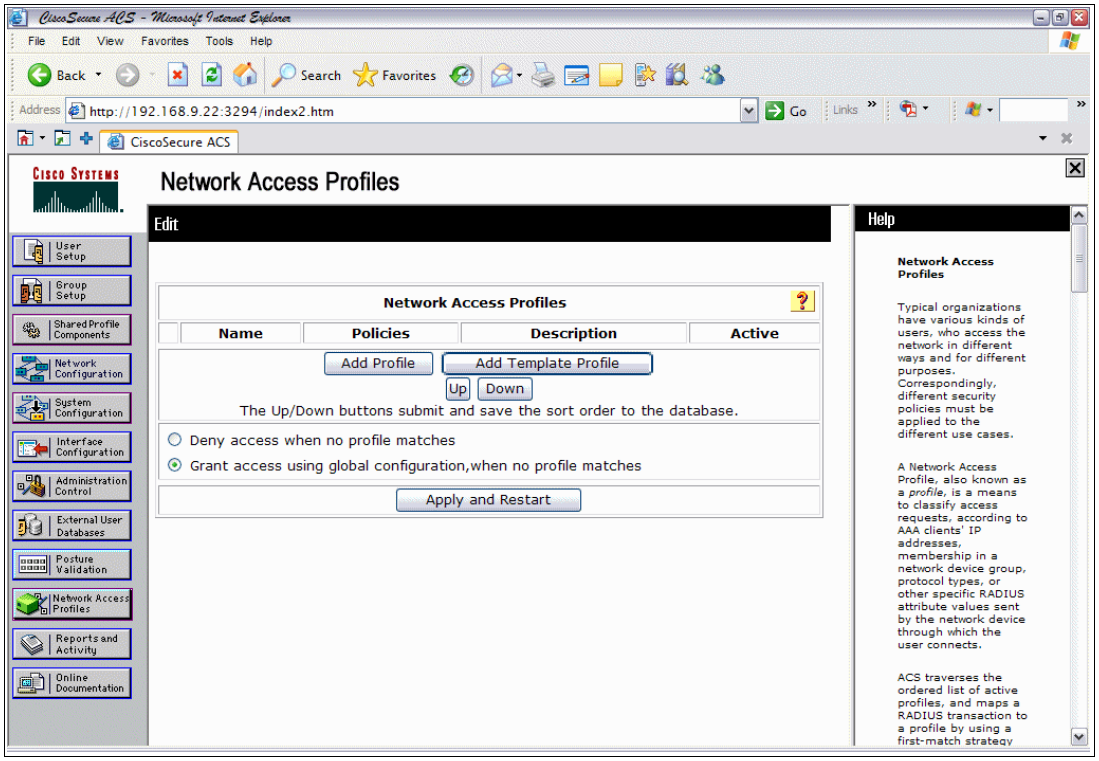

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3294/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Network Access Profiles
Name
Policies
Description
Active
Add Profile
Add Template Profile
Up
Down
The Up/Down buttons submit and save the sort order to the database.
Deny access when no profile matches
Grant access using global configuration,when no profile matches
Apply and Restart
Help
Network Access Profiles
Typical organizations have various kinds of users, who access the network in different ways and for different purposes. Correspondingly, different security policies must be applied to the different use cases.
A Network Access Profile, also known as a profile, is a means to classify access requests, according to AAA clients' IP addresses, membership in a network device group, protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.
ACS traverses the ordered list of active profiles, and maps a RADIUS transaction to a profile by using a first-match strategy

Figure 7-50 Network Access Profiles

2. Click **Add Profile**.
3. For the name, enter the name of the profile, such as `NAC_IISSCN`. Add a description and ensure that the box for Active is checked. *Allow any Protocol type* should be checked. Click **Apply and Restart**.

Downloaded from www.Manualslib.com manuals search engine

4. The newly created NAP is shown (Figure 7-51) with the three policies that comprise the NAP — *authentication*, *posture validation,* and *authorization*. Each of these will have to be configured in turn, after clicking **Apply and Restart**.

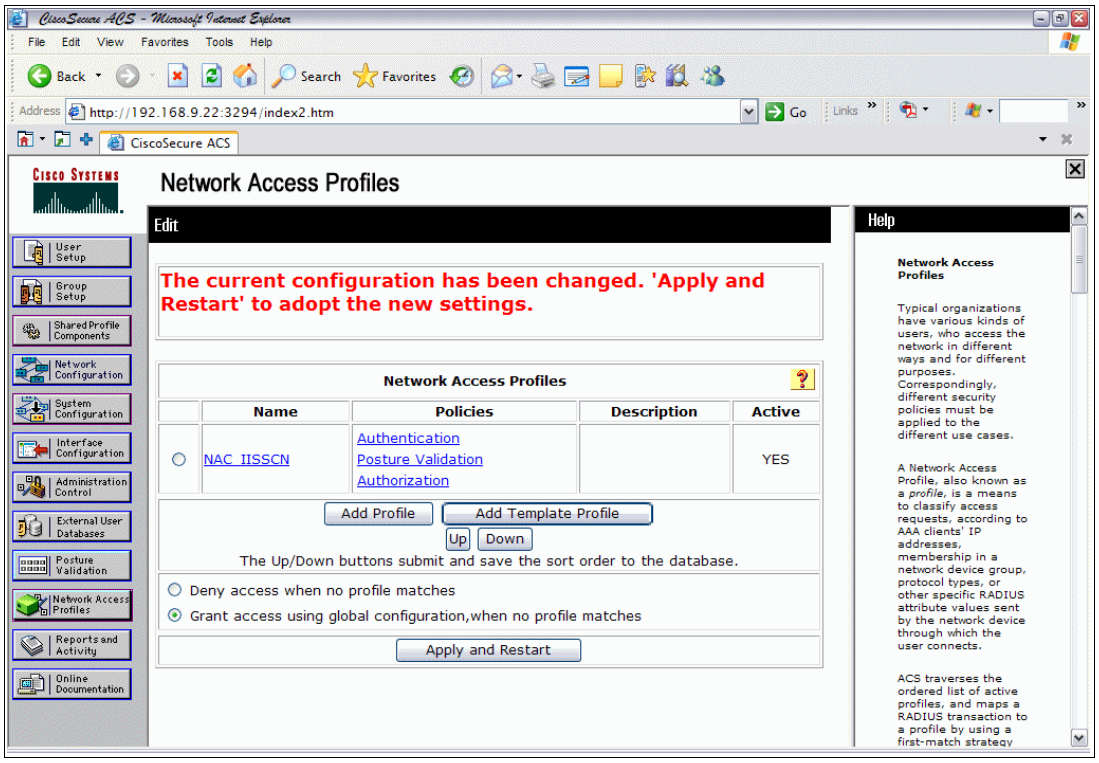

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3294/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
The current configuration has been changed. 'Apply and Restart' to adopt the new settings.
Network Access Profiles
Name
Policies
Description
Active
NAC_IISSCN
Authentication
Posture Validation
Authorization
YES
Add Profile
Add Template Profile
Up
Down
The Up/Down buttons submit and save the sort order to the database.
Deny access when no profile matches
Grant access using global configuration,when no profile matches
Apply and Restart
Help
Network Access Profiles
Typical organizations have various kinds of users, who access the network in different ways and for different purposes. Correspondingly, different security policies must be applied to the different use cases.
A Network Access Profile, also known as a profile, is a means to classify access requests, according to AAA clients' IP addresses, membership in a network device group, protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.
ACS traverses the ordered list of active profiles, and maps a RADIUS transaction to a profile by using a first-match strategy

Figure 7-51 Newly created NAP

Note: Be careful in the selection of *Deny access when no profile matches* or *Grant access using global authentication when no profile matches*. In our example, we use *Grant access....*

Downloaded from www.Manualslib.com manuals search engine

5. Click **Authentication**. Click the tab **Populate from Global** and ensure that *Posture Validation - Required* is set. *Selected Databases* should contain *ACS Internal Database* (Figure 7-52).

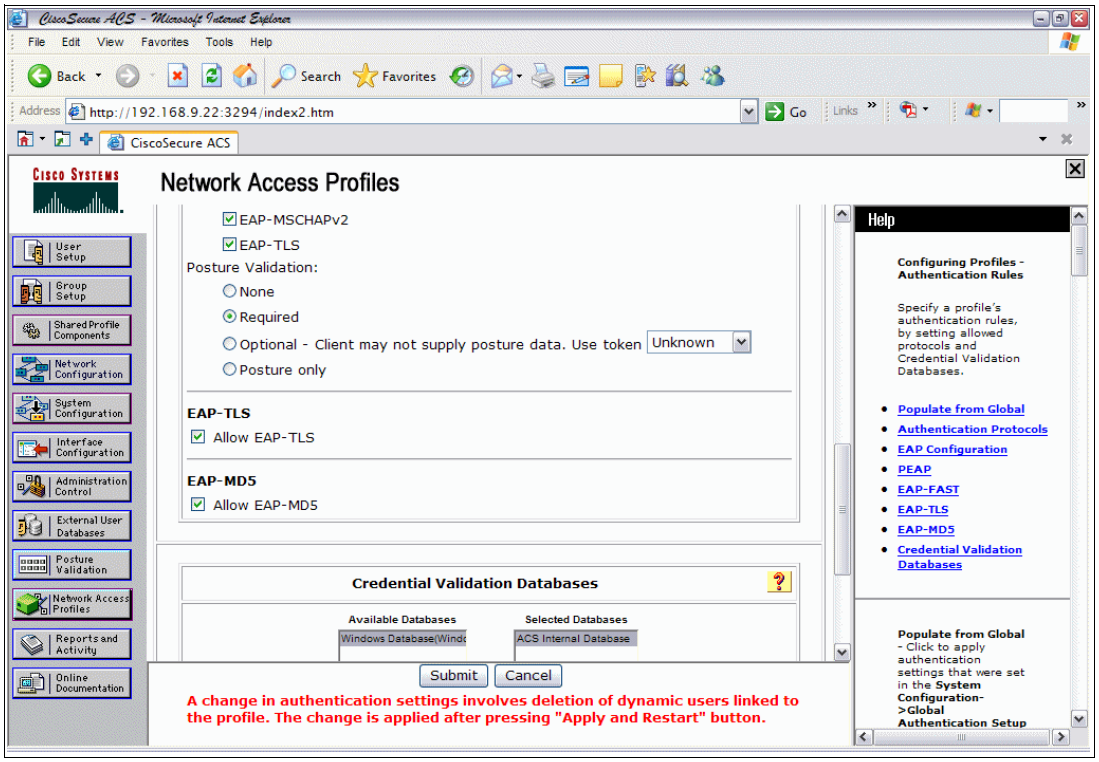


Figure 7-52 Authentication configuration for RAC

6. Click **Submit**. This will take you back to the screen in Figure 7-51 on page 272, where you will need to click **Apply and Restart**.
7. Click **Posture Validation** from the screen in Figure 7-51 on page 272.

Downloaded from www.Manualslib.com manuals search engine

8. From the screen shown in Figure 7-53, click **Add Rule**.

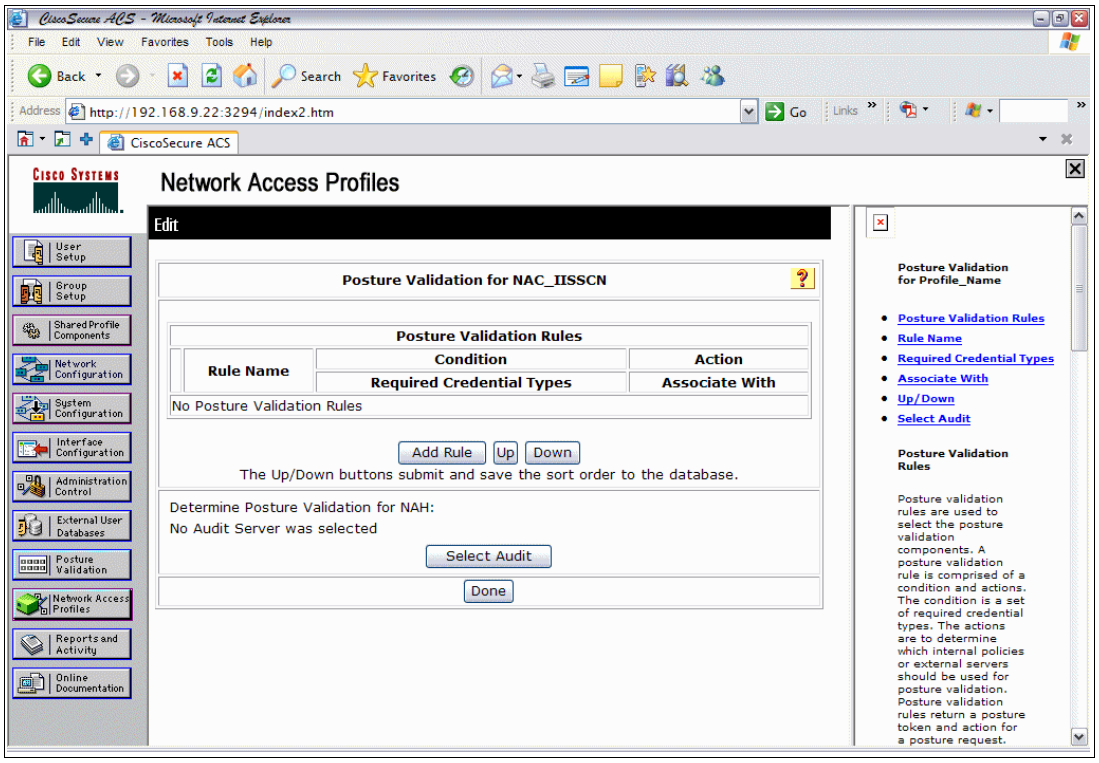

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3294/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Posture Validation for NAC_IISSCN
Posture Validation Rules
Rule Name
Condition
Action
Required Credential Types
Associate With
No Posture Validation Rules
Add Rule
Up
Down
The Up/Down buttons submit and save the sort order to the database.
Determine Posture Validation for NAH:
No Audit Server was selected
Select Audit
Done
Posture Validation for Profile_Name
Posture Validation Rules
Rule Name
Required Credential Types
Associate With
Up/Down
Select Audit
Posture Validation Rules
Posture validation rules are used to select the posture validation components. A posture validation rule is comprised of a condition and actions. The condition is a set of required credential types. The actions are to determine which internal policies or external servers should be used for posture validation. Posture validation rules return a posture token and action for a posture request.

Figure 7-53 Posture validation rule creation

9. Add a name in the Name field. In our example we used NAC_IISSCN_Posture_Profile.

Downloaded from www.Manualslib.com manuals search engine

10. Under Condition → Required Credential Types, there is a list of available credentials. Select **IBMCorporation:SCM**, then click the arrow (→) to move this to the column for selected credentials, as shown in Figure 7-54. Repeat this process for Cisco:PA (Figure 7-53 on page 274).

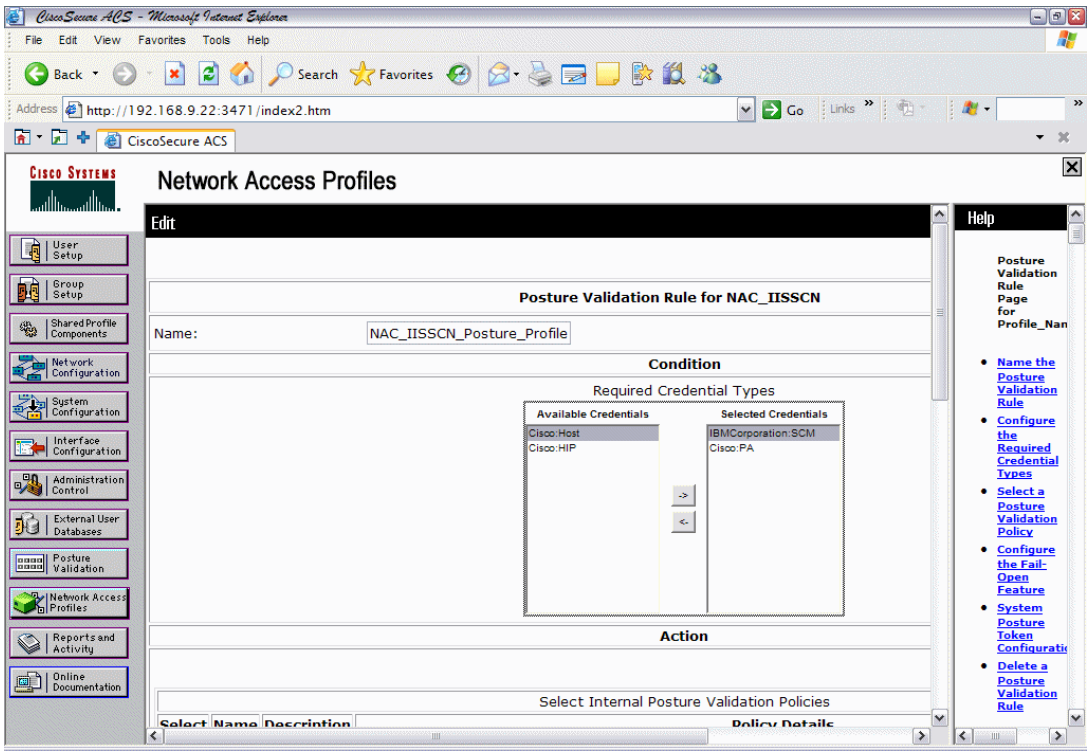


Figure 7-54 Partial configuration of posture validation

Downloaded from www.Manualslib.com manuals search engine

11. Scrolling down the page to Action → Selected Internal Posture Validation Policies, CTA and TSCM should already be present. The only action required here is to check them both under Select (Figure 7-55).

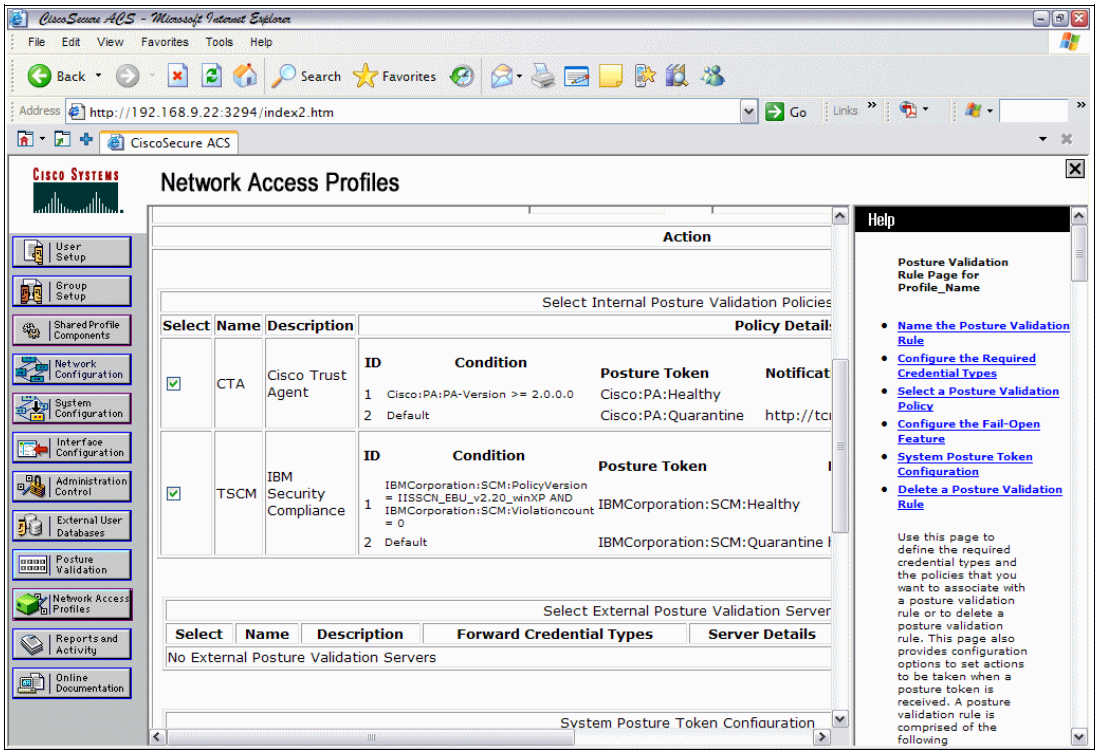

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3294/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Action
Select Internal Posture Validation Policies
Select Name Description Policy Detail
CTA Cisco Trust Agent
ID Condition Posture Token Notificat
1 Cisco:PA:PA-Version >= 2.0.0.0 Cisco:PA:Healthy
2 Default Cisco:PA:Quarantine http://tc
TSCM IBM Security Compliance
ID Condition Posture Token
1 IBMCorporation:SCM:PolicyVersion = IISSCN_EBU_v2.20_winXP AND IBMCorporation:SCM:Violationcount = 0 IBMCorporation:SCM:Healthy
2 Default IBMCorporation:SCM:Quarantine
Select External Posture Validation Server
Select Name Description Forward Credential Types Server Details
No External Posture Validation Servers
System Posture Token Configuration
Help
Posture Validation Rule Page for Profile_Name
Name the Posture Validation Rule
Configure the Required Credential Types
Select a Posture Validation Policy
Configure the Fail-Open Feature
System Posture Token Configuration
Delete a Posture Validation Rule
Use this page to define the required credential types and the policies that you want to associate with a posture validation rule or to delete a posture validation rule. This page also provides configuration options to set actions to be taken when a posture token is received. A posture validation rule is comprised of the following

Figure 7-55 Selecting CTA and TSCM policies

12. (Optional) Under *System Posture Token Configuration*, add the following syntax in the *Healthy PA message*:

```
<img border="0" src="c:\healthy.jpg"></html>
```


Downloaded from www.Manualslib.com manuals search engine

An example of the CTA Healthy pop-up is shown in Figure 7-56.

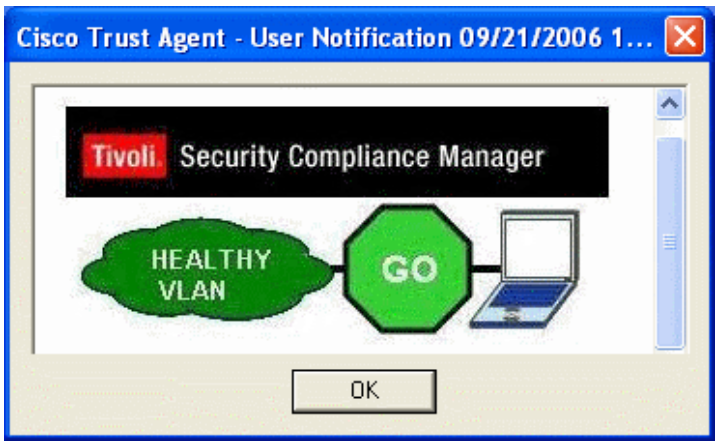


Figure 7-56 Example of CTA Healthy pop-up

13. (Optional) Under *System Posture Token Configuration*, add the following syntax in the *Quarantine PA message* (this process is depicted in Figure 7-58 on page 278):

```
<img border="0" src="c:\quarantine.jpg"></html>
```

An example of the CTA Quarantine pop-up is shown in Figure 7-57.

Figure 7-57 Example of CTA Quarantine pop-up

Downloaded from www.Manualslib.com manuals search engine

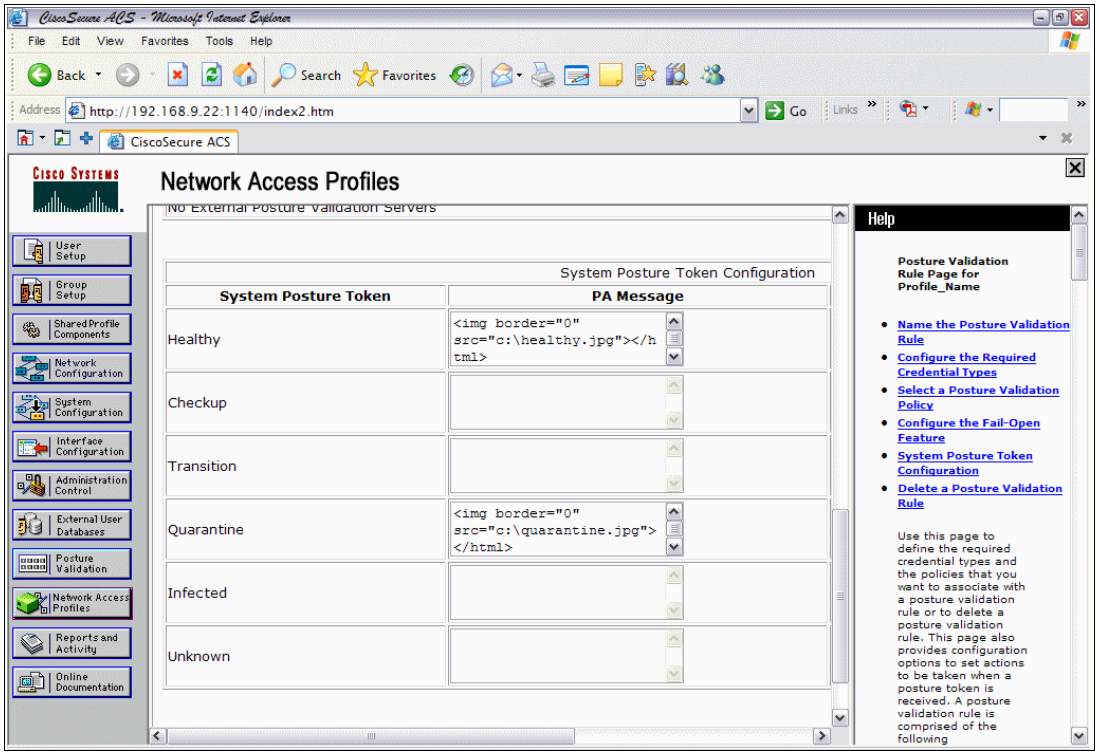

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:1140/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
System Posture Token Configuration
System Posture Token
PA Message
Healthy
<img border="0" src="c:\healthy.jpg"></html>
Checkup
Transition
Quarantine
<img border="0" src="c:\quarantine.jpg"></html>
Infected
Unknown
Help
Posture Validation Rule Page for Profile_Name
Name the Posture Validation Rule
Configure the Required Credential Types
Select a Posture Validation Policy
Configure the Fail-Open Feature
System Posture Token Configuration
Delete a Posture Validation Rule
Use this page to define the required credential types and the policies that you want to associate with a posture validation rule or to delete a posture validation rule. This page also provides configuration options to set actions to be taken when a posture token is received. A posture validation rule is comprised of the following

Figure 7-58 CTA pop-up configuration

> **Note:** Steps 12 and 13 are optional because they are simply embedding some color in the CTA pop-ups on the end user's workstation. You can tailor this so that you can have as simple or as colorful a pop-up as you like. Leaving these fields blank will result in *no* pop-up notification on the end user's screen. Note that the .jpegs referenced here must be installed in the root of the C: drive of the end user's machine. This is also customizable.

14. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

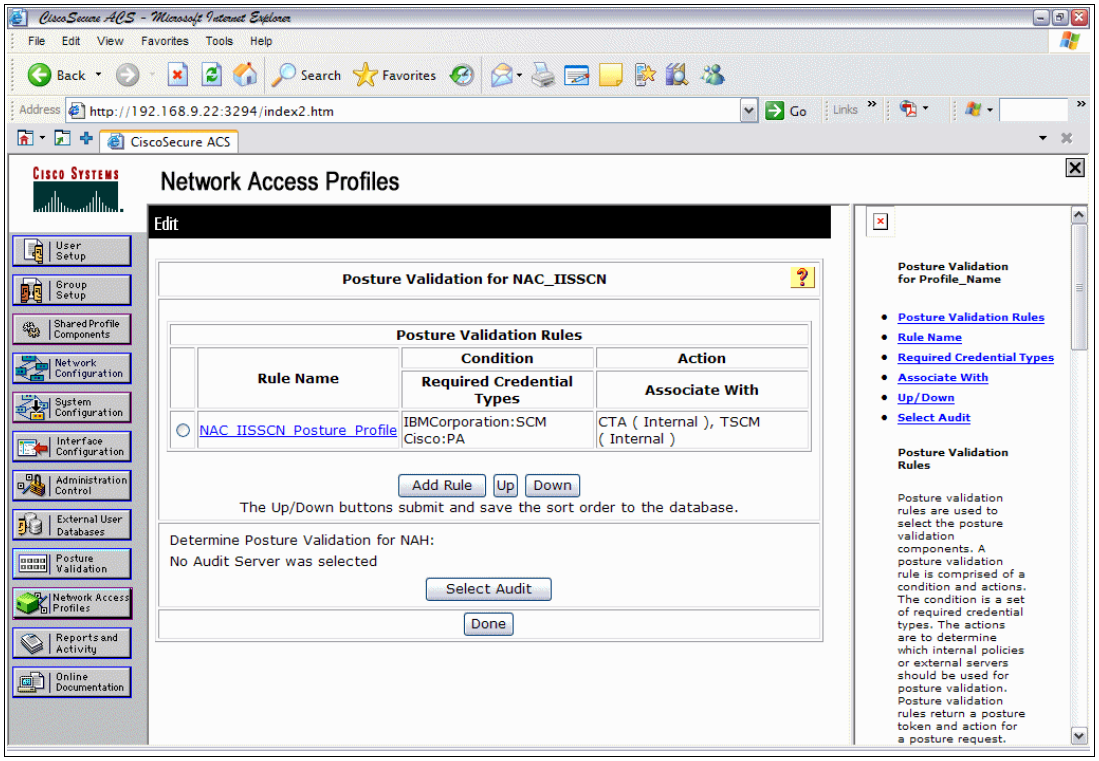


Figure 7-59 Completed posture validation for NAC_IISSCN

15. Click **Done**. This will take you back to the screen shown in Figure 7-50 on page 271. Click **Apply and Restart**.

Downloaded from www.Manualslib.com manuals search engine

16. From the screen shown in Figure 7-51 on page 272, click **Authorization**. This takes you to the dialog depicted in Figure 7-60.

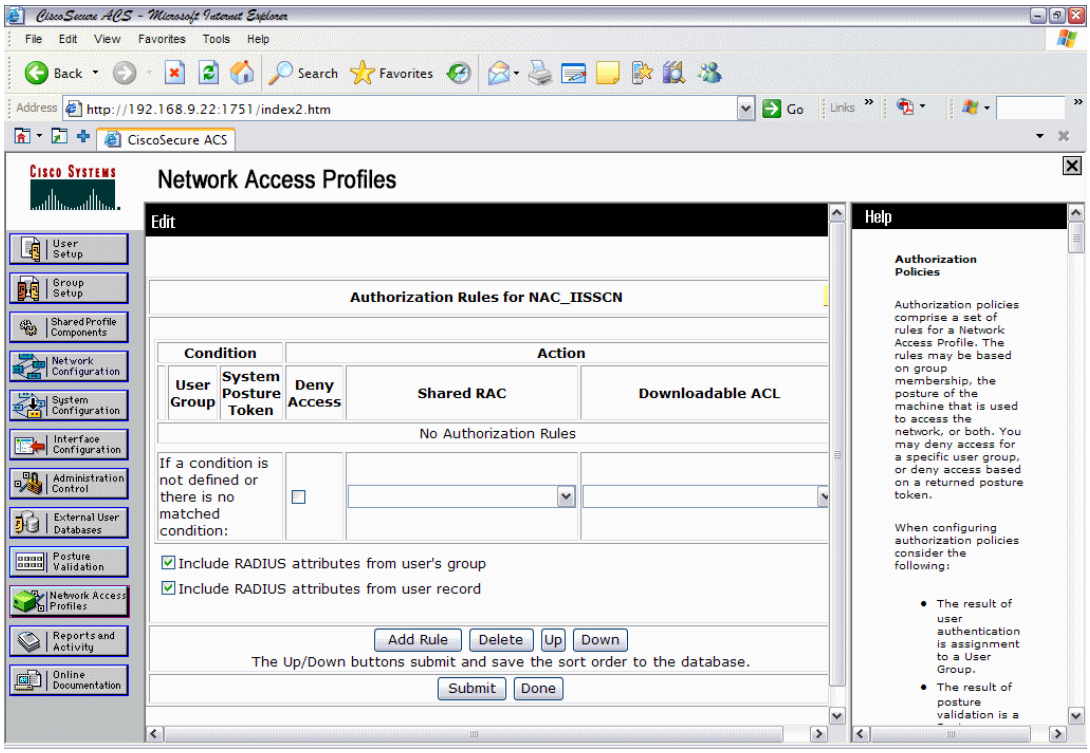

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:1751/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Authorization Rules for NAC_IISSCN
Condition
Action
User Group
System Posture Token
Deny Access
Shared RAC
Downloadable ACL
No Authorization Rules
If a condition is not defined or there is no matched condition:
Include RADIUS attributes from user's group
Include RADIUS attributes from user record
Add Rule
Delete
Up
Down
The Up/Down buttons submit and save the sort order to the database.
Submit
Done
Help
Authorization Policies
Authorization policies comprise a set of rules for a Network Access Profile. The rules may be based on group membership, the posture of the machine that is used to access the network, or both. You may deny access for a specific user group, or deny access based on a returned posture token.
When configuring authorization policies consider the following:
The result of user authentication is assignment to a User Group.
The result of posture validation is a

Figure 7-60 Authorization rule creation

17. Click **Add Rule**.
18. For this example, from the drop-down list under User Group, select **Sales**.
19. From the System Posture Token drop-down list, select **Healthy**.
20. From the Shared RAC drop-down list, select **Healthy_Sales_RAC**.

Downloaded from www.Manualslib.com manuals search engine

21. Click **Submit** (Figure 7-61).

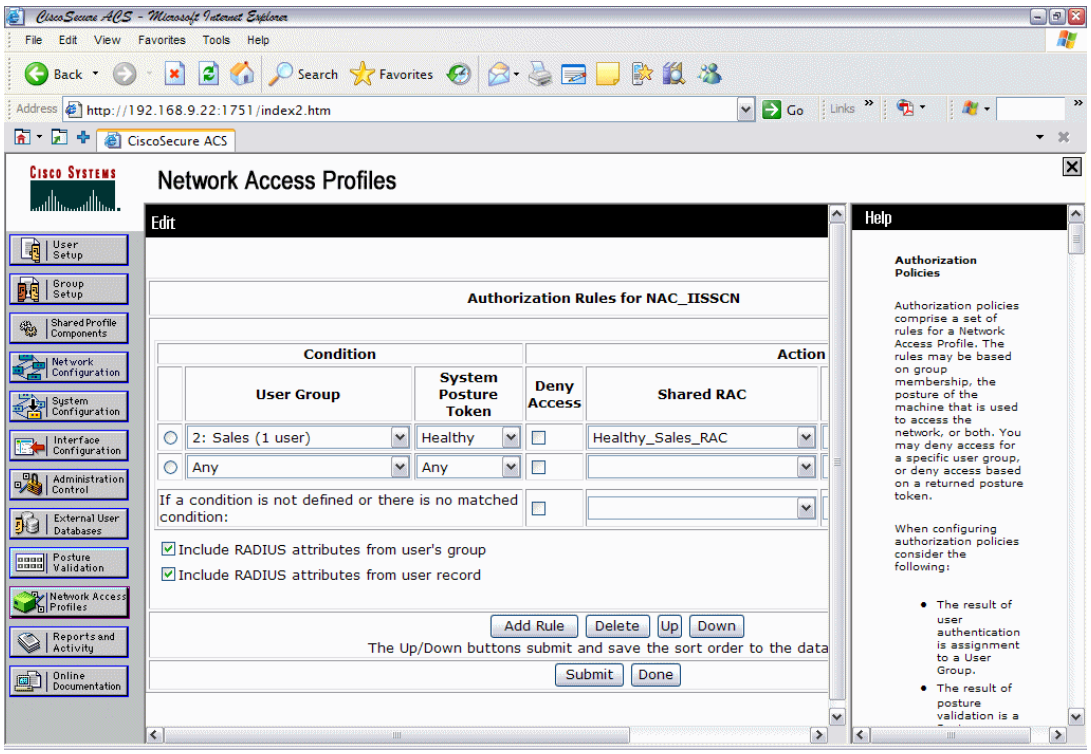

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:1751/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Authorization Rules for NAC_IISSCN
Condition
Action
User Group
System Posture Token
Deny Access
Shared RAC
2: Sales (1 user)
Healthy
Healthy_Sales_RAC
Any
Any
If a condition is not defined or there is no matched condition:
Include RADIUS attributes from user's group
Include RADIUS attributes from user record
Add Rule
Delete
Up
Down
The Up/Down buttons submit and save the sort order to the data
Submit
Done
Help
Authorization Policies
Authorization policies comprise a set of rules for a Network Access Profile. The rules may be based on group membership, the posture of the machine that is used to access the network, or both. You may deny access for a specific user group, or deny access based on a returned posture token.
When configuring authorization policies consider the following:
The result of user authentication is assignment to a User Group.
The result of posture validation is a

Figure 7-61 Healthy Sales SPT creation

> **Note:** Remember that this scenario is for NAC L2 802.1x. As mentioned previously, NAC L2 802.1x does not yet support downloadable ACLs. Therefore, the *Downloadable ACL* field has been deliberately left blank. If you were configuring NAC L2/L3 IP this field would be used. At the time that this book was written, support for NAC L2 802.1x downloadable ACLs was something to be included in future releases of Cisco IOS.

22. Repeat this process to create additional authorization rules using the information provided in Table 7-7.

Table 7-7 Authorization rules

User group	System posture token	Shared RAC
Sales	Healthy	Healthy_Sales_RAC
Sales	Quarantine	Quarantine_Sales_RAC
Engineering	Healthy	Healthy_Engineering_RAC

Downloaded from www.Manualslib.com manuals search engine

User group	System posture token	Shared RAC
Engineering	Quarantine	Quarantine_Engineering_ RAC
Condition not defined or there is no matched condition	Quarantine	Default_Quarantine_RAC

23. Your screen should look similar to that in Figure 7-62.

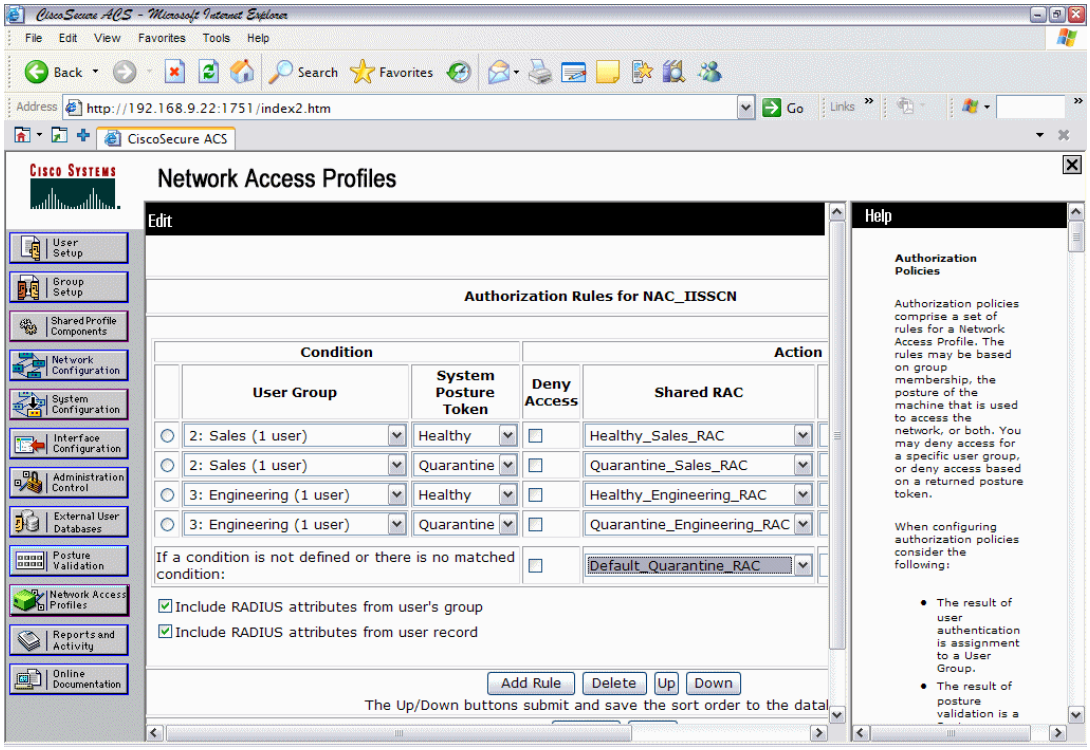


Figure 7-62 Completed Authorization RAC configuration

24. Click **Submit**.

25. This will take you back to the screen in Figure 7-51 on page 272. Click **Apply and Restart**.

Downloaded from www.Manualslib.com manuals search engine

External User Database

One of the most common methods of deploying an ACS is to use an external user database, such as Active Directory, or using a token server, for user and machine authentication. We did not use this method in the writing of this book. However, should you require information about how to do this, please refer to the following URL:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_user_guide_chapter09186a008052e944.html

Unknown user policy

There are a few different scenarios for the *unknown user*. In the simplest sense, an unknown user is one that does not have a valid user account, either on the ACS (if it is providing the authentication) or on an external user database, such as Microsoft Active Directory, but has the CTA with supplicant installed. In this case, the user will be prompted to enter their dot1x credentials, which will of course fail. This is by design, and the user will be kept off the network. The way to address this is that the user would have to log a call with the Helpdesk to have her account created or recreated.

Clientless user

If a client tries to connect who does not have the CTA installed in a NAC L2 802.1x environment, there is no way to authenticate them via dot1x, nor is there any way to validate their posture. It does not matter whether they have a valid user account, as there is no way that their credentials can get to the ACS. The way to address this issue is to use the *guest-vlan* option in the switch configuration on all NAC-enabled switches. In our scenario, this was VLAN15, our *default Quarantine* VLAN. The access lists applied to this VLAN allowed for DNS and Internet access only. All other traffic is denied. Note that *all of the configuration for this is done on the switch*. There is nothing to do on the ACS. Once the user has an IP address for the guest-vlan, there will be an entry in the ACS under *Failed Attempts*.

This concludes the details for the Cisco Secure ACS server configuration for NAC L2 802.1x.

7.1.2 Configuring the Cisco Secure ACS for NAC L2/L3 IP

This section documents the changes that must be made to the previous section to configure the ACS for a NAC deployment using L2IP or L3 *without* IEEE 802.1x.

Downloaded from www.Manualslib.com manuals search engine

Downloadable Access Control Lists

NAC L2/L3 IP uses EAPoUDP (EOU), which allows for ACLs to be *downloaded* from the ACS to the NAD. In our example, the NAD will be a Cisco 3750 switch. The ACLs are downloaded on a per-user basis and are applied to the individual switch ports on a per-session basis. The section describes how to configure these downloadable ACLs.

1. From the main menu, select **System Configuration**.
2. From System Configuration, select **Downloadable IP ACLs**.
3. We have deleted all the sample ACLs to go through the process of creating them from scratch (Figure 7-63).

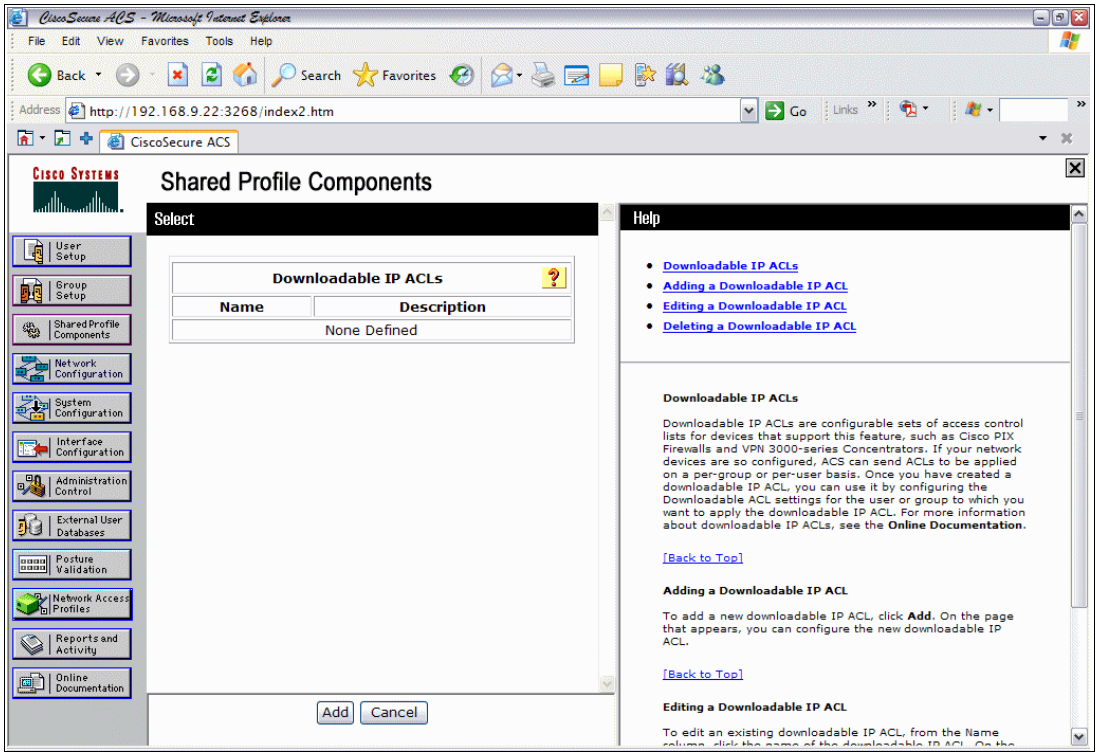

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:3268/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Shared Profile Components
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Downloadable IP ACLs
Name
Description
None Defined
Add
Cancel
Help
Downloadable IP ACLs
Adding a Downloadable IP ACL
Editing a Downloadable IP ACL
Deleting a Downloadable IP ACL
Downloadable IP ACLs
Downloadable IP ACLs are configurable sets of access control lists for devices that support this feature, such as Cisco PIX Firewalls and VPN 3000-series Concentrators. If your network devices are so configured, ACS can send ACLs to be applied on a per-group or per-user basis. Once you have created a downloadable IP ACL, you can use it by configuring the Downloadable ACL settings for the user or group to which you want to apply the downloadable IP ACL. For more information about downloadable IP ACLs, see the Online Documentation.
[Back to Top]
Adding a Downloadable IP ACL
To add a new downloadable IP ACL, click Add. On the page that appears, you can configure the new downloadable IP ACL.
[Back to Top]
Editing a Downloadable IP ACL

Figure 7-63 Downloadable ACL creation

4. Click **Add**.

Downloaded from www.Manualslib.com manuals search engine

5. Add a name and description in the Name and Description fields as appropriate (Figure 7-64). After this has been done, click **Add**.

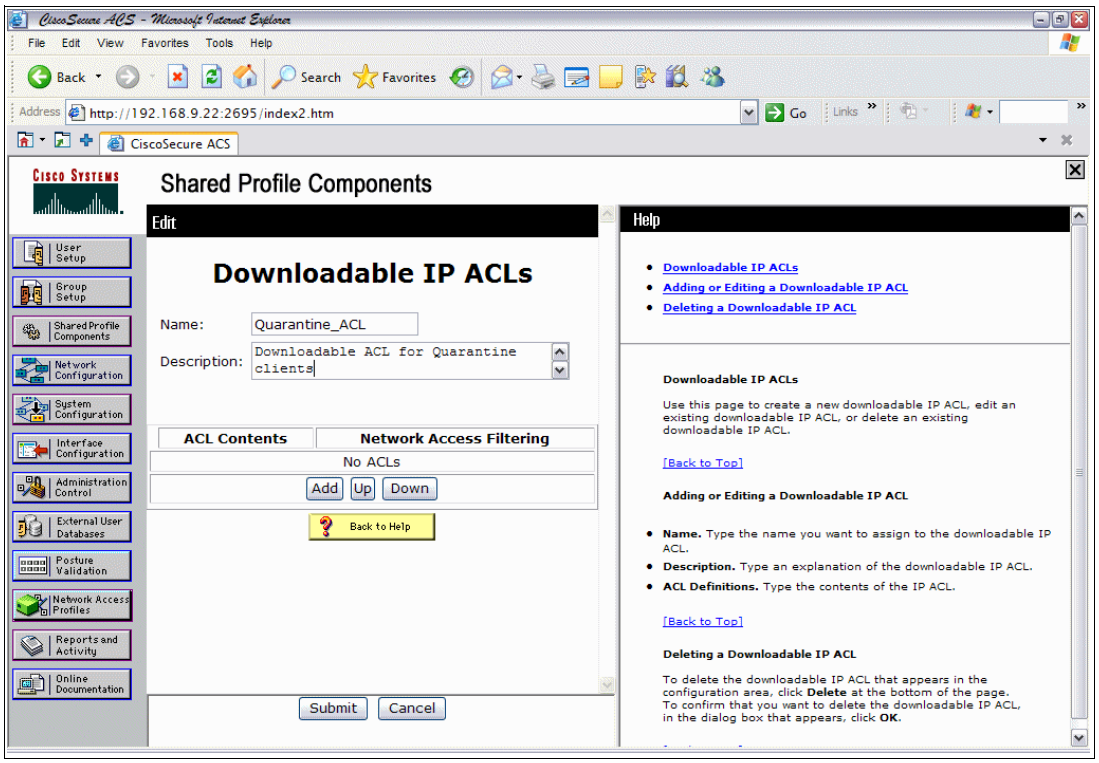

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:2695/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Shared Profile Components
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Downloadable IP ACLs
Name: Quarantine_ACL
Description: Downloadable ACL for Quarantine clients
ACL Contents
Network Access Filtering
No ACLs
Add Up Down
Back to Help
Submit Cancel
Help
Downloadable IP ACLs
Adding or Editing a Downloadable IP ACL
Deleting a Downloadable IP ACL
Downloadable IP ACLs
Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.
[Back to Top]
Adding or Editing a Downloadable IP ACL
Name. Type the name you want to assign to the downloadable IP ACL.
Description. Type an explanation of the downloadable IP ACL.
ACL Definitions. Type the contents of the IP ACL.
[Back to Top]
Deleting a Downloadable IP ACL
To delete the downloadable IP ACL that appears in the configuration area, click Delete at the bottom of the page. To confirm that you want to delete the downloadable IP ACL, in the dialog box that appears, click OK.

Figure 7-64 Naming of ACL

Downloaded from www.Manualslib.com manuals search engine

6. Enter the name of the ACL and the ACL definition (Figure 7-65).

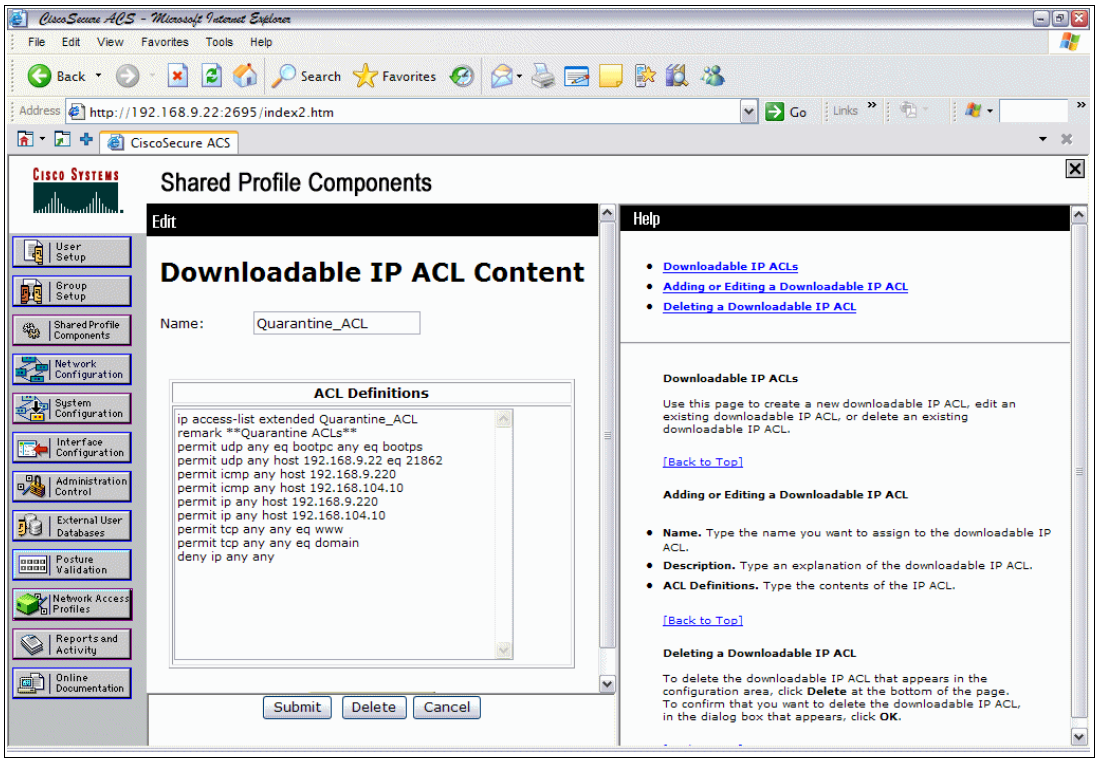

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:2695/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Shared Profile Components
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Downloadable IP ACL Content
Name: Quarantine_ACL
ACL Definitions
ip access-list extended Quarantine_ACL
remark **Quarantine ACLs**
permit udp any eq bootpc any eq bootps
permit udp any host 192.168.9.22 eq 21862
permit icmp any host 192.168.9.220
permit icmp any host 192.168.104.10
permit ip any host 192.168.9.220
permit ip any host 192.168.104.10
permit tcp any any eq www
permit tcp any any eq domain
deny ip any any
Submit Delete Cancel
Help
Downloadable IP ACLs
Adding or Editing a Downloadable IP ACL
Deleting a Downloadable IP ACL
Downloadable IP ACLs
Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.
[Back to Top]
Adding or Editing a Downloadable IP ACL
Name. Type the name you want to assign to the downloadable IP ACL.
Description. Type an explanation of the downloadable IP ACL.
ACL Definitions. Type the contents of the IP ACL.
[Back to Top]
Deleting a Downloadable IP ACL
To delete the downloadable IP ACL that appears in the configuration area, click Delete at the bottom of the page. To confirm that you want to delete the downloadable IP ACL, in the dialog box that appears, click OK.

Figure 7-65 Quarantine ACL definitions

7. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

8. Note that there is an option of binding the ACL just created to a network access filter (Figure 7-66). This allows for different ACLs to be applied to different items. We are not using network filtering, so we leave the default (All-AAA-Clients).

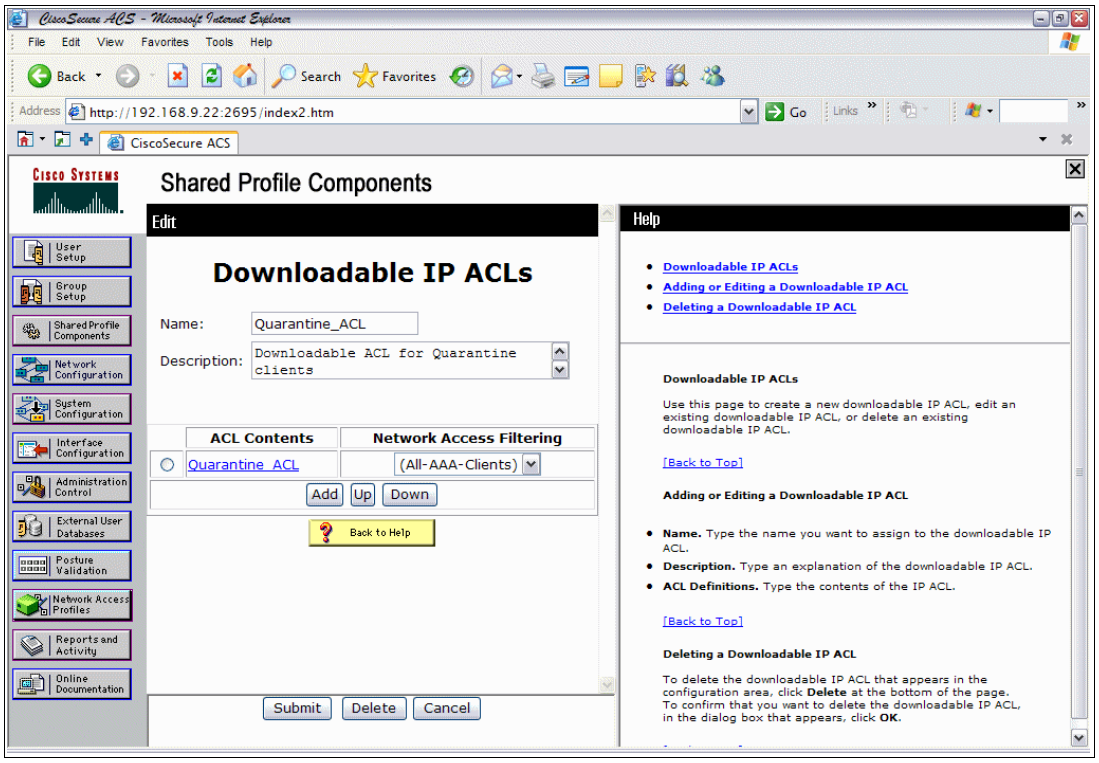

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:2695/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Shared Profile Components
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Downloadable IP ACLs
Name: Quarantine_ACL
Description: Downloadable ACL for Quarantine clients
ACL Contents
Network Access Filtering
Quarantine_ACL
(All-AAA-Clients)
Add Up Down
Back to Help
Submit Delete Cancel
Help
Downloadable IP ACLs
Adding or Editing a Downloadable IP ACL
Deleting a Downloadable IP ACL
Downloadable IP ACLs
Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.
[Back to Top]
Adding or Editing a Downloadable IP ACL
Name. Type the name you want to assign to the downloadable IP ACL.
Description. Type an explanation of the downloadable IP ACL.
ACL Definitions. Type the contents of the IP ACL.
[Back to Top]
Deleting a Downloadable IP ACL
To delete the downloadable IP ACL that appears in the configuration area, click Delete at the bottom of the page. To confirm that you want to delete the downloadable IP ACL, in the dialog box that appears, click OK.

Figure 7-66 Binding the ACL

9. Click **Submit**.
10. Repeat steps 4–9 for the various ACLs to be created. In our example, we only use *Healthy* and *Quarantine*, with *Healthy* being a *permit ip any*.

Configuring RADIUS Authorization Components

To do this:

1. Select **Shared Profile Components** from the main menu.
2. Select **RADIUS Authorization Components**.

Downloaded from www.Manualslib.com manuals search engine

3. Repeat step 3 on page 265 to step 12 on page 268, using the values listed in Table 7-8 and Table 7-9. We used the names Healthy_L2IP_RAC and Quarantine_L2IP_RAC.

Note: These values are *instead of* the values listed previously, as opposed to *in addition to*.

Table 7-8 L2 IP Healthy RAC values

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=healthy_hosts
Cisco IOS/PIX 6.0	cisco-av-pair (1)	url-redirect-acl=healthy_acl
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)

Table 7-9 L2 IP Quarantine RAC values

Vendor	Attribute	Value
Cisco IOS/PIX 6.0	cisco-av-pair (1)	status-query-timeout=30
Cisco IOS/PIX 6.0	cisco-av-pair (1)	sec:pg=quarantine_hosts
Cisco IOS/PIX 6.0	cisco-av-pair (1)	url-redirect-acl=quarantine_acl
IETF	Session-Timeout (27)	3600
IETF	Termination-Action (29)	RADIUS-Request(1)

Note: The name of the ACL specified in the *url-redirect-acl* attribute must be configured on the switch. It is case-sensitive and must match exactly. If it does not match, it will not function on the switch. The syntax of the ACL must be identical also. We suggest using extended access lists.

Downloaded from www.Manualslib.com manuals search engine

Configuring Network Access Profiles

We have now configured all the individual components to be in a position to bring them together and create the Network Access Profiles, which determine what to check and what action to take based on the results of those checks. Again, we have deleted all the pre-configured sample configs to create our own from scratch.

1. Repeat step 1 on page 271 through to step 18 on page 280 (Figure 7-67).

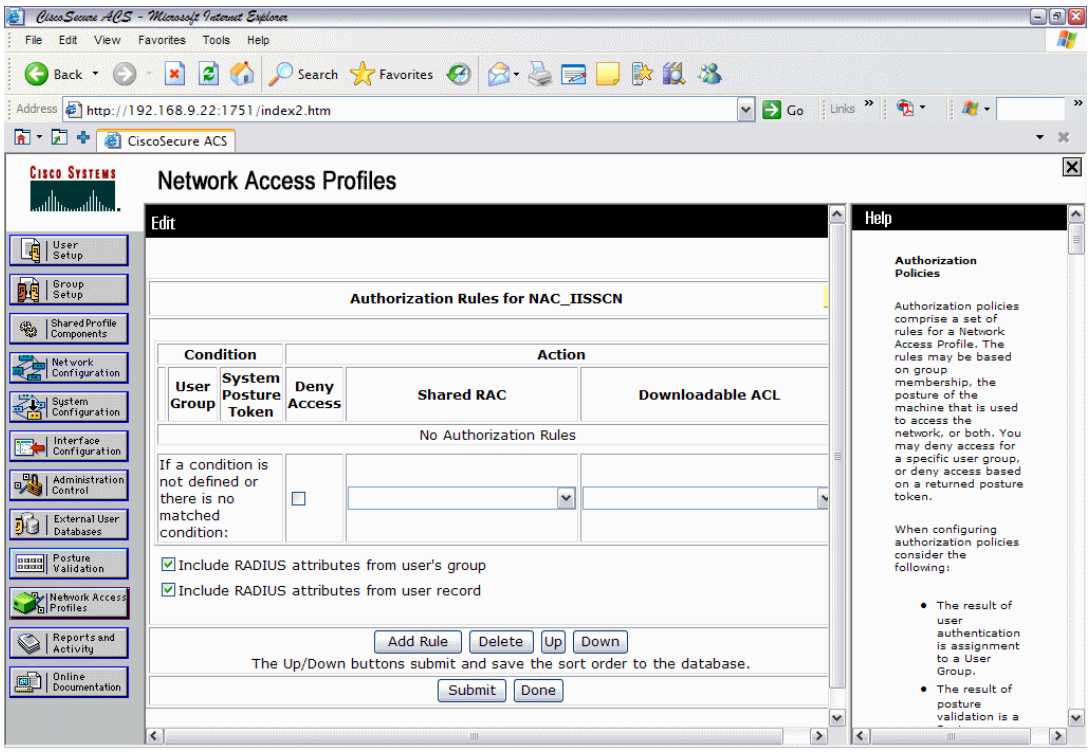

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.9.22:1751/index2.htm
Go Links
CiscoSecure ACS
Cisco Systems
Network Access Profiles
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
Authorization Rules for NAC_IISSCN
Condition
Action
User Group
System Posture Token
Deny Access
Shared RAC
Downloadable ACL
No Authorization Rules
If a condition is not defined or there is no matched condition:
Include RADIUS attributes from user's group
Include RADIUS attributes from user record
Add Rule
Delete
Up
Down
The Up/Down buttons submit and save the sort order to the database.
Submit
Done
Help
Authorization Policies
Authorization policies comprise a set of rules for a Network Access Profile. The rules may be based on group membership, the posture of the machine that is used to access the network, or both. You may deny access for a specific user group, or deny access based on a returned posture token.
When configuring authorization policies consider the following:
The result of user authentication is assignment to a User Group.
The result of posture validation is a

Figure 7-67 Ready to create Authorization rules

2. Click **Add Rule**.
3. From the User Group drop-down list, select **Any**.
4. From the System Posture Token drop-down list, select **Healthy**.
5. From the Shared RAC drop-down list, select **Healthy_L2IP_RAC**.

Downloaded from www.Manualslib.com manuals search engine

6. From the Downloadable ACL drop-down list, select **Healthy_ACL** (Figure 7-68).

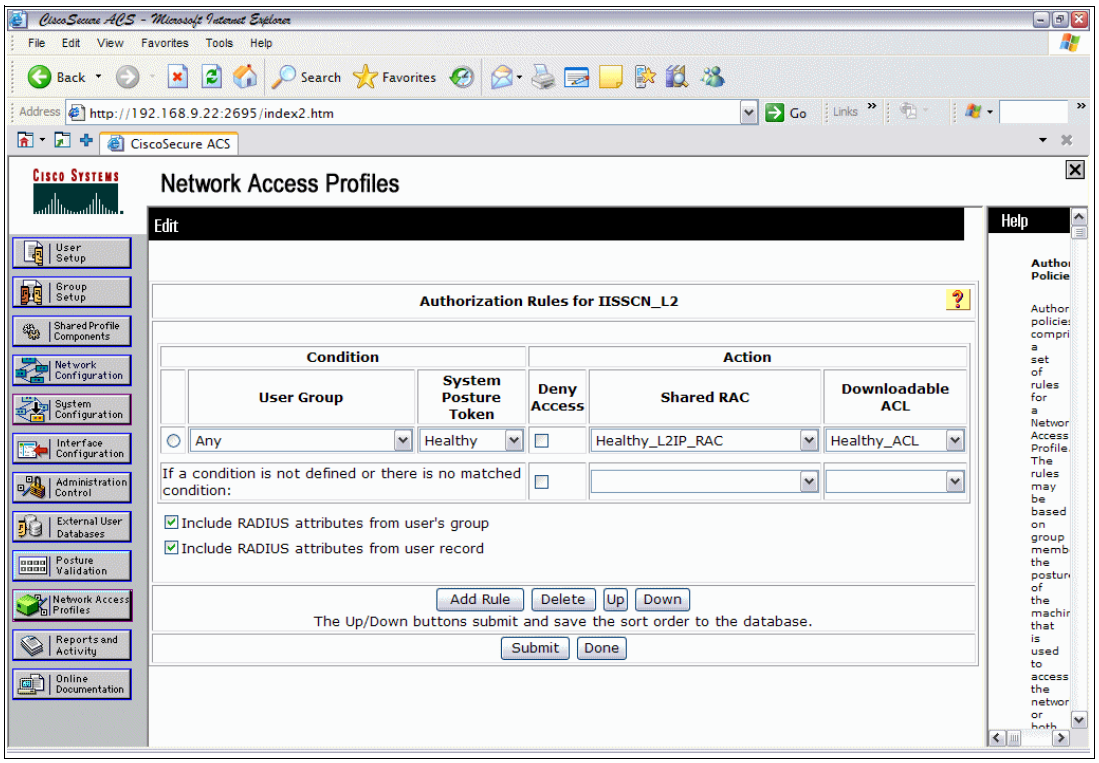


Figure 7-68 L2IP Healthy Authorization rule

7. Click **Add Rule**.
8. From User Group, select **Any**.
9. From System Posture Token, select **Quarantine**.
10. From Shared RAC, select **Quarantine_L2IP_RAC**.
11. From Downloadable ACL, select **Quarantine_ACL**.

Downloaded from www.Manualslib.com manuals search engine

12. For this scenario, we selected the Quarantine_L2IP_RAC and Quarantine_ACL as the Shared RAC and Downloadable ACL to be applied in case a condition is not defined or there is no matched condition (Figure 7-69).

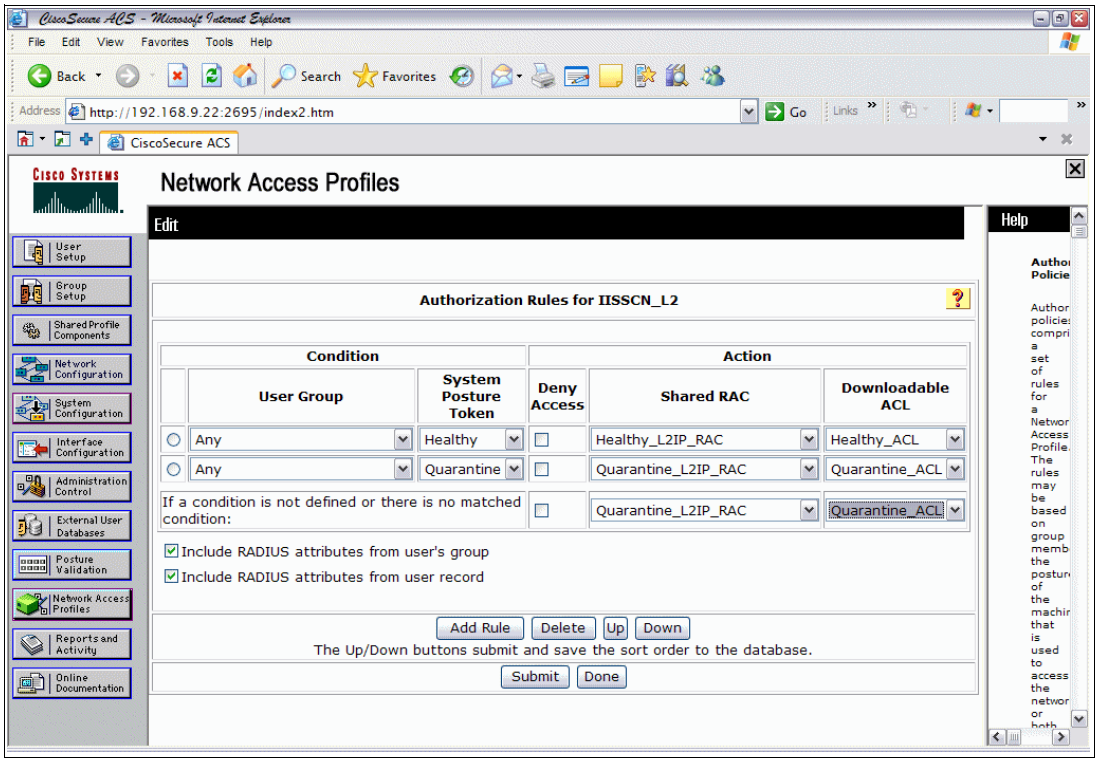


Figure 7-69 Completed L2IP Authorization rules

13. Click **Submit**.

14. Click **Apply and Restart**.

This concludes the changes that needed to be made to the previous section to configure the ACS for a NAC deployment using L2IP or L3 *without* IEEE 802.1x.

7.1.3 Deployment of the network infrastructure

In this section we describe how to configure the Cisco Catalyst 3750 switch acting as the NAD for both NAC L2 802.1x and NAC L2 IP implementations, and a Cisco IOS router for NAC L3 IP implementation.

Downloaded from www.Manualslib.com manuals search engine

Configuring Cisco 3750 switch for NAC L2 802.1x

New for NAC Phase 2 is the ability of a Cisco switch to act as a NAC policy enforcement device. For the purposes of this book, we used a Cisco 3750 switch, running the Advanced IP Services Version 12.2(25) SEE2 version of IOS.

```
Switch   Ports  Model          SW Version            SW Image
*    1      26  WS-C3750-24P   12.2(25)SEE2          C3750-ADVIPSERVICESK
```

Our example is using L2Dot1x. The protocol used in this architecture is EAPOL, as opposed to EAPoUDP (EOU). For this reason, there is no EOU configuration required on the switch, just a straightforward dot1x configuration. We recommend that you check the Cisco Web site for the latest hardware/software compatibility matrixes, as this could determine which deployments of NAC are available to you. For example, at the time of writing this book, a Cisco 2950 switch supports NAC L2 802.1x, but *not* NAC L2/L3 IP (no support for EoU). Another example is that a Cisco 6500 running 12.2(18)SXF does *not* support NAC L2 802.1x authentication and validation on edge switches.

The current switch compatibility matrix can be found at:

http://www.cisco.com/en/US/partner/netsol/ns617/networking_solutions_documentation_roadmap09186a008066499c.html#wp1016600

Note: Always thoroughly document the environment on which you wish to deploy this solution. You may find that the environment is either already compatible or requires IOS upgrades or hardware upgrades.

The basic switch configuration is listed below:

```
aaa new-model
aaa authentication login local_only line
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
ip routing
!
dot1x system-auth-control
!
ip radius source-interface Vlan9
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server host 192.168.9.22 auth-port 1645 acct-port 1646
radius-server source-ports 1645-1646
radius-server key cisco123
radius-server vsa send authentication
```


Downloaded from www.Manualslib.com manuals search engine

```
!
<output omitted>
!
interface FastEthernet1/0/5
 description **Connected to CARE-SYSTEM Workstation**
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout reauth-period server
 dot1x reauthentication
 dot1x guest-vlan 15
 spanning-tree portfast
!
<output omitted>
```

The Access Controls Lists (ACLs) that we used in our scenario are listed below:

```
access-list 110 remark **Healthy Sales VLAN ACLs**
access-list 110 deny ip any 192.168.13.0 0.0.0.255
access-list 110 deny ip any 192.168.14.0 0.0.0.255
access-list 110 deny ip any 192.168.15.0 0.0.0.255
access-list 110 permit ip any any
!
access-list 120 remark **Healthy Engineering VLAN ACLs**
access-list 120 deny ip any 192.168.13.0 0.0.0.255
access-list 120 deny ip any 192.168.14.0 0.0.0.255
access-list 120 deny ip any 192.168.15.0 0.0.0.255
access-list 120 permit ip any any
!
access-list 130 remark **Quarantine Sales VLAN ACLs**
access-list 130 permit icmp any host 192.168.9.220
access-list 130 permit icmp any host 192.168.104.10
access-list 130 permit ip any host 192.168.9.220
access-list 130 permit ip any host 192.168.104.10
access-list 130 permit udp any eq bootpc any eq bootps
access-list 130 deny ip any 192.168.11.0 0.0.0.255
access-list 130 deny ip any 192.168.12.0 0.0.0.255
access-list 130 deny ip any 192.168.14.0 0.0.0.255
access-list 130 deny ip any 192.168.15.0 0.0.0.255
access-list 130 permit tcp any any eq www
access-list 130 permit tcp any any eq domain
access-list 130 deny ip any any log
!
access-list 140 remark **Quarantine Engineering VLAN ACLs**
access-list 140 permit icmp any host 192.168.9.220
access-list 140 permit icmp any host 192.168.104.10
access-list 140 permit ip any host 192.168.9.220
access-list 140 permit ip any host 192.168.104.10
access-list 140 permit udp any eq bootpc any eq bootps
```


Downloaded from www.Manualslib.com manuals search engine

```
access-list 140 deny ip any 192.168.11.0 0.0.0.255
access-list 140 deny ip any 192.168.12.0 0.0.0.255
access-list 140 deny ip any 192.168.13.0 0.0.0.255
access-list 140 deny ip any 192.168.15.0 0.0.0.255
access-list 140 permit tcp any any eq www
access-list 140 permit tcp any any eq domain
access-list 140 deny ip any any
!
access-list 150 remark **Default Quarantine VLAN ACLs**
access-list 150 deny ip any 192.168.11.0 0.0.0.255
access-list 150 deny ip any 192.168.12.0 0.0.0.255
access-list 150 deny ip any 192.168.13.0 0.0.0.255
access-list 150 deny ip any 192.168.14.0 0.0.0.255
access-list 150 permit udp any eq bootpc any eq bootps
access-list 150 permit tcp any any eq www
access-list 150 permit tcp any any eq domain
access-list 150 deny ip any any
```

Note: When you enable AAA for IEEE 802.1x, it is automatically enabled for all lines and interfaces. Unless some other method of line authentication is enabled for console, aux or tty, the username and password for IEEE 802.1x must be used. If you use the command **`aaa authentication login default none`**, no authentication is required for login. Unless you specify a local username/password combination, or have some other method of local authentication enabled, you will be *locked out of the console* when you exit.

The reasoning behind these ACLs is as follows:

- Healthy

  If you are in either of the healthy VLANs, you should not be able to communicate with anything that is in any of the quarantine VLANs, but you should have full access to the rest of the network.

- Quarantine

  a. If you are in either the sales or engineering Quarantine VLAN, you will need access to a DHCP server to get an IP address.

  b. You should be able to ping the Security Compliance Manager and Tivoli Configuration Manager to test communication to them to ensure that this is not the reason that you are in quarantine.

  c. Allowing full IP connectivity to these two servers allows for a new policy to be downloaded from the Security Compliance Manager or a remediation workflow to occur from the Tivoli Configuration Manager.

  d. You should not be able to communicate with any other host outside of the respective quarantine VLAN that you are in, other than the Security Compliance Manager and Tivoli Configuration Manager. We did, however,

Downloaded from www.Manualslib.com manuals search engine

allow Web access and DNS access in case of manual remediation requirements or access to the intranet Web pages for help.

On the 3750 switch, enter the following verification command:

show dot1x interface fa1/0/5 detail

```
nac3750sa#sho dot1x interface fa1/0/5 detail

Dot1x Info for FastEthernet1/0/5
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = (From Authentication Server)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Guest-Vlan                = 15

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0011.25ce.f56c
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE

Port Status               = AUTHORIZED
ReAuthPeriod              = 60
ReAuthAction              = Reauthenticate
TimeToNextReauth          = 59
Authentication Method     = Dot1x
Posture                   = Quarantine
Authorized By             = Authentication Server
Vlan Policy               = 13
```

A full NAC Framework documentation reference guide can be found at:

http://www.cisco.com/en/US/partner/netsol/ns617/networking_solutions_documentation_roadmap09186a008066499c.html

Configuring Cisco 3750 switch for NAC L2 IP

See “Configuring Cisco 3750 switch for NAC L2 802.1x” on page 292 for prerequisites.

Downloaded from www.Manualslib.com manuals search engine

Note: Both NAC L2 802.1x and NAC L2 IP configurations can be supported on the same switch. Similarly, the authorization setup under Network Access Profiles can be configured to support both NAC L2 802.1x clients and NAC L2 IP clients. This allows you to have a hybrid environment, using one ACS.

This section describes how to configure a Cisco 3750 switch acting as the NAD:

```
aaa new-model
aaa authentication login local_only line
aaa authentication eou default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
!
ip admission name l2-lpip eapoudp
!
ip device tracking
!
eou timeout hold-period 61
eou timeout status-query 60
eou timeout retransmit 7
eou timeout revalidation 60
eou logging
identity profile eapoudp
!
<output omitted>
interface FastEthernet1/0/11
 description **L2IP Test Port**
 switchport access vlan 11
 switchport mode access
 ip access-group initial-acl in
 spanning-tree portfast
 ip admission l2-lpip
!
<output omitted>
!
ip access-list extended Healthy_ACL
 remark **Healthy ACL**
 permit ip any any
ip access-list extended Quarantine_ACL
 remark **Quarantine ACLs**
 permit udp any eq bootpc any eq bootps
 permit udp any host 192.168.9.22 eq 21862
 permit icmp any host 192.168.9.220
 permit icmp any host 192.168.104.10
 permit ip any host 192.168.9.220
 permit ip any host 192.168.104.10
 permit tcp any any eq www
```


Downloaded from www.Manualslib.com manuals search engine

```
 permit tcp any any eq domain
 deny   ip any any
ip access-list extended initial-acl
 permit udp any any eq domain
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit icmp any any
 permit udp any any eq 21862
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server host 192.168.9.22 auth-port 1645 acct-port 1646
radius-server source-ports 1645-1646
radius-server key cisco123
radius-server vsa send authentication
!
```

On the 3750 switch, enter the following verification commands.

show eou all to verify the client's current status:

```
nac3750sa#show eou all
-------------------------------------------------------------------------
Address         Interface           AuthType   Posture-Token Age(min)
-------------------------------------------------------------------------
192.168.11.51   FastEthernet1/0/11  EAP        Quarantine      0
```

show ip access-list interface fa1/0/11 to check that the downloadable ACL has been applied to the switchport:

```
nac3750sa#sho ip access-list interface fa1/0/11
IP Admission access control entires (Inbound)
     permit udp host 192.168.11.51 eq bootpc any eq bootps
     permit udp host 192.168.11.51 host 192.168.9.22 eq 21862
     permit icmp host 192.168.11.51 host 192.168.9.220
     permit icmp host 192.168.11.51 host 192.168.104.10
     permit ip host 192.168.11.51 host 192.168.9.220
     permit ip host 192.168.11.51 host 192.168.104.10
     permit tcp host 192.168.11.51 any eq www
     permit tcp host 192.168.11.51 any eq domain
     deny ip host 192.168.11.51 any
nac3750sa#
```

show eou ip 192.168.11.51 to see a summary of that particular host:

```
nac3750sa#sho eou ip 192.168.11.51
Address              : 192.168.11.51
MAC Address          : 0011.25ce.f56c
Interface            : FastEthernet1/0/11
AuthType             : EAP
```


Downloaded from www.Manualslib.com manuals search engine

```
Audit Session ID    : 000000005222BFF40000001BC0A80B33
PostureToken        : Quarantine
Age(min)            : 0
URL Redirect        : NO URL REDIRECT
URL Redirect ACL    : Quarantine_ACL
ACL Name            : #ACSACL#-IP-Quarantine_ACL-4514163a
User Name           : CARE-SYSTEM:Markus
Revalidation Period : 3600 Seconds
Status Query Period : 30 Seconds
Current State       : AUTHENTICATED
```

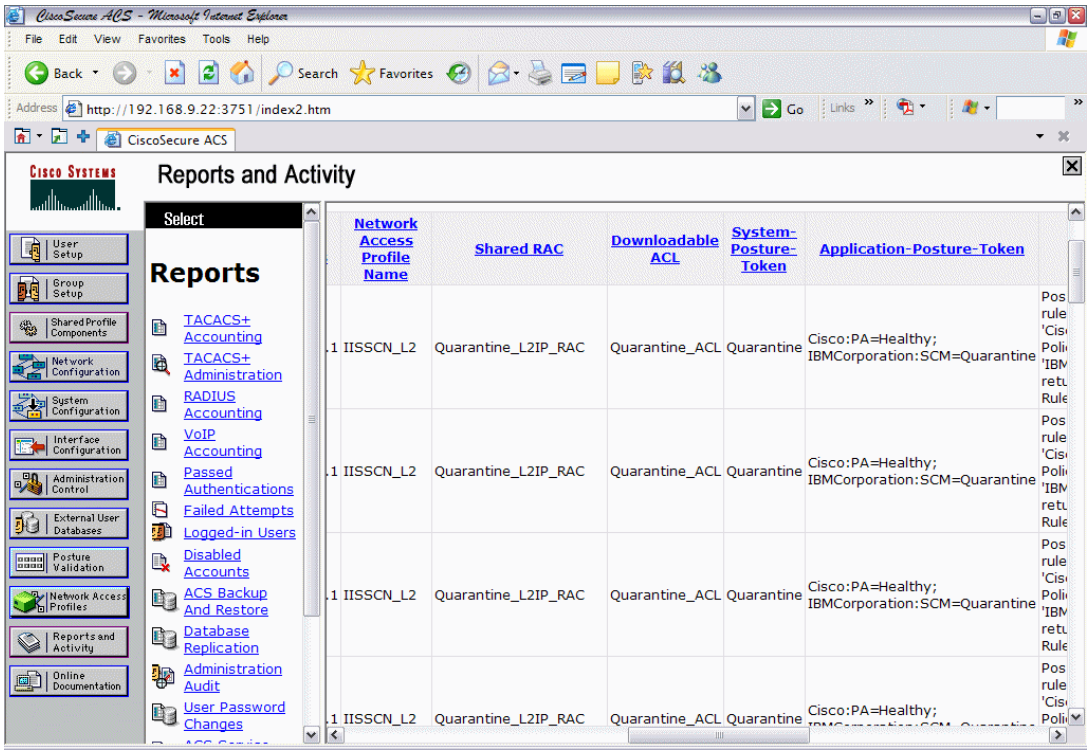


Figure 7-70 Corresponding Passed Authentications screen from the ACS

Configuring Cisco IOS Router for NAC L3 IP

Currently, NAC requires a Cisco IOS Software router running Cisco IOS Software Release 12.3(8)T or later that includes the Cisco IOS Advanced Security feature. The current router compatibility matrix can be found at:

http://www.cisco.com/en/US/partner/netsol/ns617/networking_solutions_documentation_roadmap09186a008066499c.html#wp1008583

This section describes how to configure the Cisco IOS Software device acting as the NAD, which includes these steps:

1. Configuring AAA EOU Authentication Protocols and Authentication Proxy Authorization Protocols, AAA Setup, RADIUS Server Host and Key

Downloaded from www.Manualslib.com manuals search engine

2. Configuring Admission Control EOU
3. Configuring an Exception List Configuration for Clientless Hosts
4. Configuring Clientless User Policy
5. Configuring EAP over UDP Timers
6. Configuring the Interfaces and Intercept ACL
7. Configuring the HTTP Server
8. Enabling EOU Logging

For more information, see the Cisco IOS Software Release 12.3(8)T new features documentation specific to NAC at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_nac.htm

1. To set up AAA for EAPoUDP (EOU), perform the following commands using your router command console:

```
Router(config)# aaa new-model
Router(config)# aaa authentication eou default group radius
Router(config)# aaa session-id common
Router(config)# radius-server host 10.1.1.1 key secret
```

Replace the word *secret* with the shared key you configured for the Cisco Secure ACS. Also configure the source IP address interface for the RADIUS packets that were configured in the Cisco Secure ACS network configuration.

Attention: If AAA is not already configured and you configure it now, you could be locked out of the router without configuring a way for the person to log in.

Tip: For redundancy, you can configure multiple RADIUS server entries.

2. Enable the EOU posture validation process.

   To specify that any packet received on the interface to which this policy is applied triggers the admission control process, use:

   ```
   Router(config)# ip admission name admission-name eapoudp
   ```

   Replace *admission-name* as appropriate.

   Optionally, you can exempt traffic from triggering the admission control process by applying an ACL to the NAC policy statement in the configuration.

Downloaded from www.Manualslib.com manuals search engine

This example causes traffic with a destination port 53 (domain) or port 21862 (default EAP-over-UDP) to be exempt from the admission control process:

```
Router(config)# access-list 102 deny udp any host 10.10.30.10 eq 21862
Router(config)# access-list 102 deny udp any host 10.10.20.10 eq domain
Router(config)# access-list 102 permit ip any any
Router(config)# ip admission name admission-name eapoudp list 102
```

These packets need a corresponding entry in the interface ACL to be successfully forwarded without a prior posture validation taking place. No posture validation triggering occurs if only `deny` statements are present in the intercept ACL.

3. (optional) If hosts with a statically configured IP address and no posture agent installed (non-responsive hosts) are located in the network where posturing is taking place, they may be exempted from the posturing process.

   The following commands configure a policy that enables access defined by an access list to a host with a static IP address. (Be aware that the four lines following `identity policy NACless` are actually part of the identity policy configuration and not the global router configuration.)

   ```
   Router(config)# identity profile eapoudp
   Router(config)# device authorize ip-address 172.30.40.32 policy NACless
   Router(config)# identity policy NACless
   Router(config)# access-group clientException
   Router(config)# redirect url http://172.30.2.10/update
   Router(config)# ip access-list extended clientException
   Router(config)# permit ip any host 172.30.1.10
   ```

   This configuration enables a host with an IP address of 172.30.40.32 to communicate with the host 172.30.1.10 and no other hosts. This configuration is useful for IP-connected printers or IP telephony devices.

   In the case of networks where only Web clients exist, URL redirection can point those clients to a server where the appropriate software can be obtained.

4. This section describes a different exception method for hosts without a posture agent installed.

   In the following example, the **`eou clientless username`** command configures the Cisco IOS Software NAD to insert a user name of *clientless* for clientless end stations in the RADIUS protocol. The **`eou clientless password`** command configures the password to be returned. The **`eou allow clientless`** command enables the return of the previous user name-password combination for all hosts the NAD attempts to posture without receiving a valid EOU response.

   ```
   Router(config)# eou clientless username clientless
   Router(config)# eou clientless password password
   Router(config)# eou allow clientless
   ```


Downloaded from www.Manualslib.com manuals search engine

The Cisco Secure ACS then issues a token according to the group in which a user with the clientless user name is placed. This configuration is useful for PCs and workstations that receive their IP addresses through DHCP and do not have the posture agents installed.

5. (optional) The following commands configure the timers for the EOU posturing processes. These timers are shown with their default settings:

```
Router(config)# eou timeout hold-period 60
Router(config)# eou timeout revalidation 1800
Router(config)# eou timeout status-query 300
```

The **eou timeout hold-period** command specifies a hold period in seconds for ignoring packets from a host that has just unsuccessfully authenticated. The **eou timeout revalidation** command sets the global revalidation period for all clients. This may be overridden by a RADIUS AV pair from the Cisco Secure ACS. The **eou timeout status-query** command sets the global status query period. This may also be overridden by an AV pair received from the Cisco Secure ACS.

6. The network interface configuration consists of two commands that must be configured on the interface facing the hosts to be posture-validated.

```
Router(config)# access-list 101 permit udp any host 172.30.40.1 eq 21862
Router(config)# access-list 101 deny ip any any
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 172.30.40.1 255.255.255.0
Router(config-if)# ip access-group 101 in
Router(config-if)# ip admission admission-name
```

The **ip access-group 101 in** command places an ACL on the interface in the inbound direction that blocks all traffic, unless expressly permitted, from entering the interface. This ACL, called the interface ACL, is useful for creating pin holes that allow certain kinds of inbound traffic before subjecting that device to the posturing process.

For example, an access control element (ACE) permitting UDP packets equal to domain enables DNS queries to be sent successfully without being postured. The interface ACL at a minimum must permit inbound UDP communication destined to port 21862. The first permit ACE enables this UDP traffic into the NAD. This is necessary for the EOU communications. The **ip admission *admission-name*** command applies the previously configured NAC policy to the interface.

The traffic specifically permitted by access list 102 is subject to the posturing process.

Important: Remember the importance of permitting UDP port 21862 in the Interface ACL. Without this access, NAC will not function.

Downloaded from www.Manualslib.com manuals search engine

7. Enabling the HTTP server is necessary for URL redirection. When URL redirection is configured in the group configuration section, these URL redirections are sent to the Cisco IOS Software NAD.

```
Router(config)# ip http server
Router(config)# ip http authentication aaa
Router(config)# no ip http secure-server
```

8. This command enables EAPoUDP system logging from the Cisco IOS Software NAD to the console:

```
Router(config)# eou logging
```

Verifying Network Admission Control

To verify EAP and EAPoUDP messages or sessions, enter the **show eou** or **show eou all** command. Example 7-3 shows sample output.

Example 7-3 Output of show eou and show eou all command

```
Router# show eou
Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Enabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 180 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Enabled
Clientless Host Username = clientless
Clientless Host Password = password
Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface FastEthernet0/0
No interface specific configuration

Router# show eou all
-------------------------------------------------------------------
Address         Interface       AuthType   Posture-Token Age(min)
-------------------------------------------------------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
10.3.3.30       FastEthernet0/0 EAP        Healthy        13
10.3.3.31       FastEthernet0/0 EAP        Quarantine      2

Router#
```

7.2 Configuring NAC Appliance components

There are various components that make up the NAC Appliance solution. They are:

- Clean Access Manager (CAM) - The administrative server for Clean Access deployment. The secure Web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment. For out-of-band deployment, the Web admin console also provides Switch Management capability.
- Clean Access Server (CAS) - Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM Web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Clean Access system requirements. It can be deployed in-band or out-of-band. The CAS can be deployed in the following ways:
  - In-band Virtual Gateway (L2 transparent bridging mode)
  - In-band Real-IP Gateway
  - In-band NAT Gateway (IP router/default gateway with NAT services)
  - Out-of-band Virtual Gateway
  - Out-of-band Real-IP Gateway
  - Out-of-band NAT Gateway

  For the purposes of this book, we focus on out-of-band Virtual Gateway (OOB VG).
- Clean Access Agent (CAA) - Optional read-only agent that resides on Windows clients. The Clean Access Agent checks applications, files, services, or registry keys to ensure that clients meet your specified network and software requirements prior to gaining access to the network.

Downloaded from www.Manualslib.com manuals search engine

7.2.1 Installing CCA Agent

At the time of writing this book, the latest version of the CCA Agent available from Cisco was 4.0.2.0. The version that we used for this book is a special Version 4.0.1.1.

Note: This version of the CCA Agent is supplied with the downloadable files for this book. See Appendix C, “Additional material” on page 481, for more details on how to obtain this file.

1. Click **CCAAgent_Setup.exe**. Click **Next** in the screen shown in Figure 7-71.

Cisco Clean Access Agent - InstallShield Wizard
Welcome to the InstallShield Wizard for Cisco Clean Access Agent
The InstallShield(R) Wizard will install Cisco Clean Access Agent 4.0.1.1 on your computer. To continue, click Next.
Clean Access Agent
by Cisco Systems
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Figure 7-71 Installation wizard

Downloaded from www.Manualslib.com manuals search engine

2. Accept the default installation folder and click **Next**, as shown in Figure 7-72.

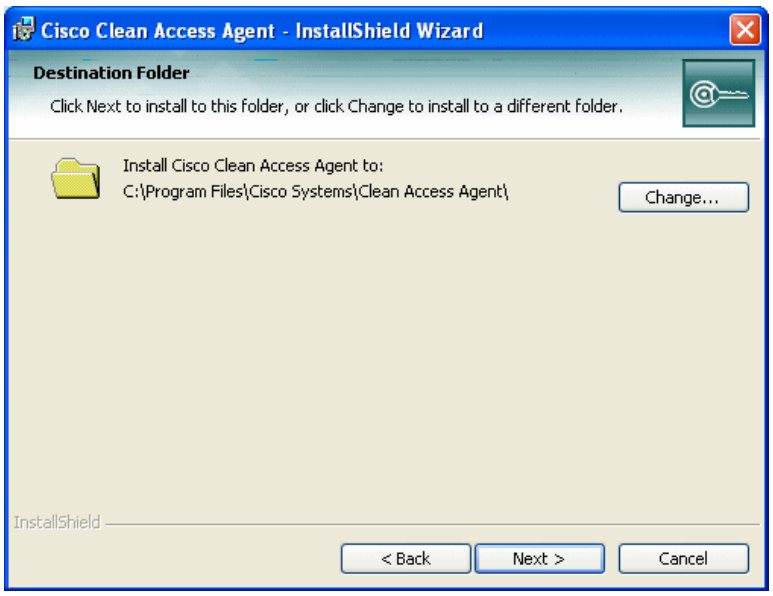

Cisco Clean Access Agent - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Cisco Clean Access Agent to:
C:\Program Files\Cisco Systems\Clean Access Agent\
Change...
InstallShield
< Back
Next >
Cancel

Figure 7-72 Default install directory

3. Click **Install** to begin the installation (Figure 7-73).

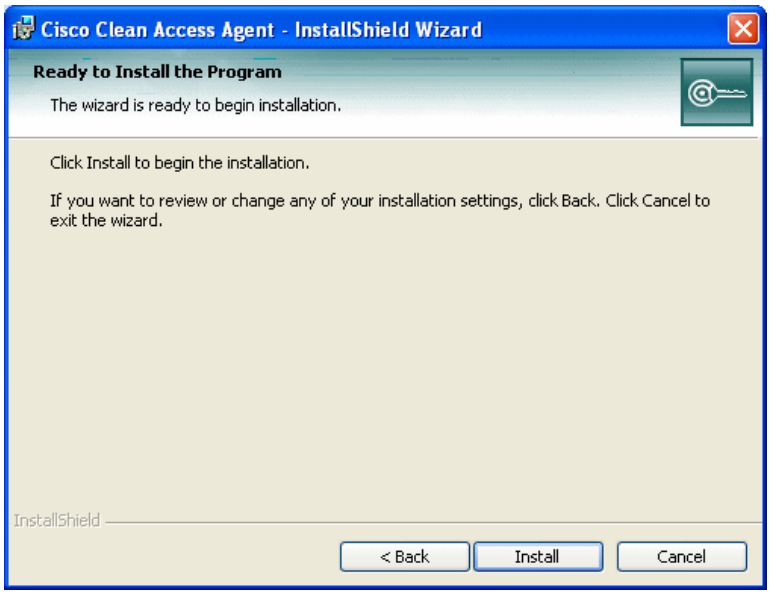

Cisco Clean Access Agent - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

Figure 7-73 Beginning the installation

Downloaded from www.Manualslib.com manuals search engine

4. Click **Finish** to complete the installation (Figure 7-74).

Cisco Clean Access Agent - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Cisco Clean Access Agent. Click Finish to exit the wizard.
Clean Access Agent
by Cisco Systems
< Back
Finish
Cancel

Figure 7-74 Completed installation

7.2.2 Configuring a CCA OOB VG server

The CAM uses Java Remote Method Invocation (RMI) for parts of its communication with the CAS, which means it uses dynamically allocated ports for this purpose. For deployments that have a firewall between the CAS and the CAM, we recommend setting up rules in the firewall that allow communication between the CAS and the CAM (bi-directional) on the ports shown in Table 7-10.

Table 7-10 TCP port requirements for firewalls

CCA version	Required ports
3.6(x)	TCP ports 80, 443, 1099, 8995, 8996
3.5(x)	TCP ports 80, 443, 1099, 32768–61000

Downloaded from www.Manualslib.com manuals search engine

The steps are:

1. Open a Web browser and enter the IP address of the CAM. There is no specific port required.
2. Enter the administrator name and password, then click **Login** (Figure 7-75).

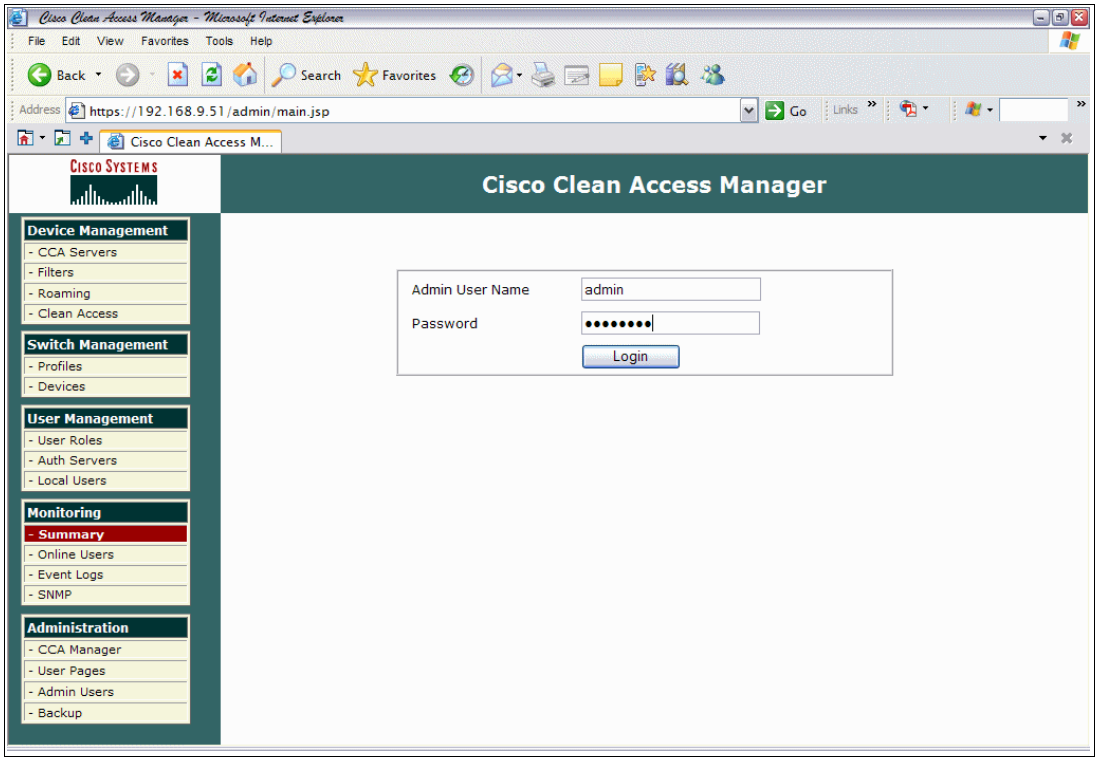


Figure 7-75 CAM login page

Downloaded from www.Manualslib.com manuals search engine

3. The Clean Access Summary window will be displayed (Figure 7-76).

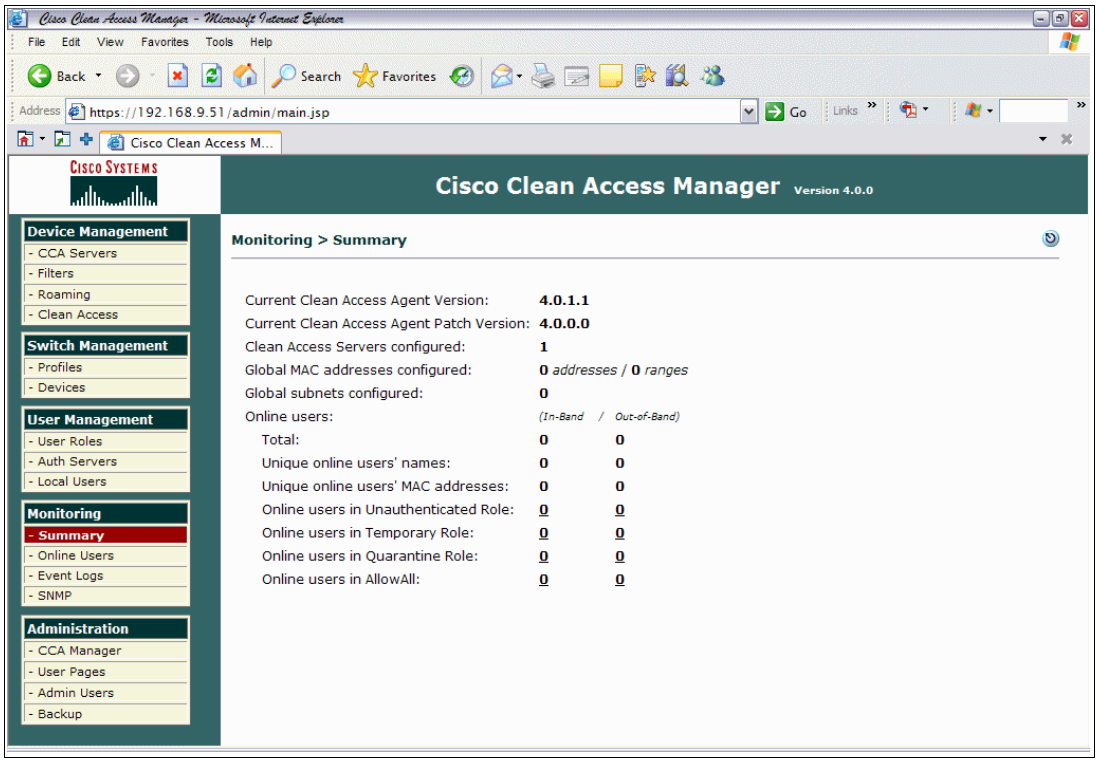


Figure 7-76 CAM summary window

Downloaded from www.Manualslib.com manuals search engine

4. From the Main Menu, select **Device Management → CCA Servers** (Figure 7-77).

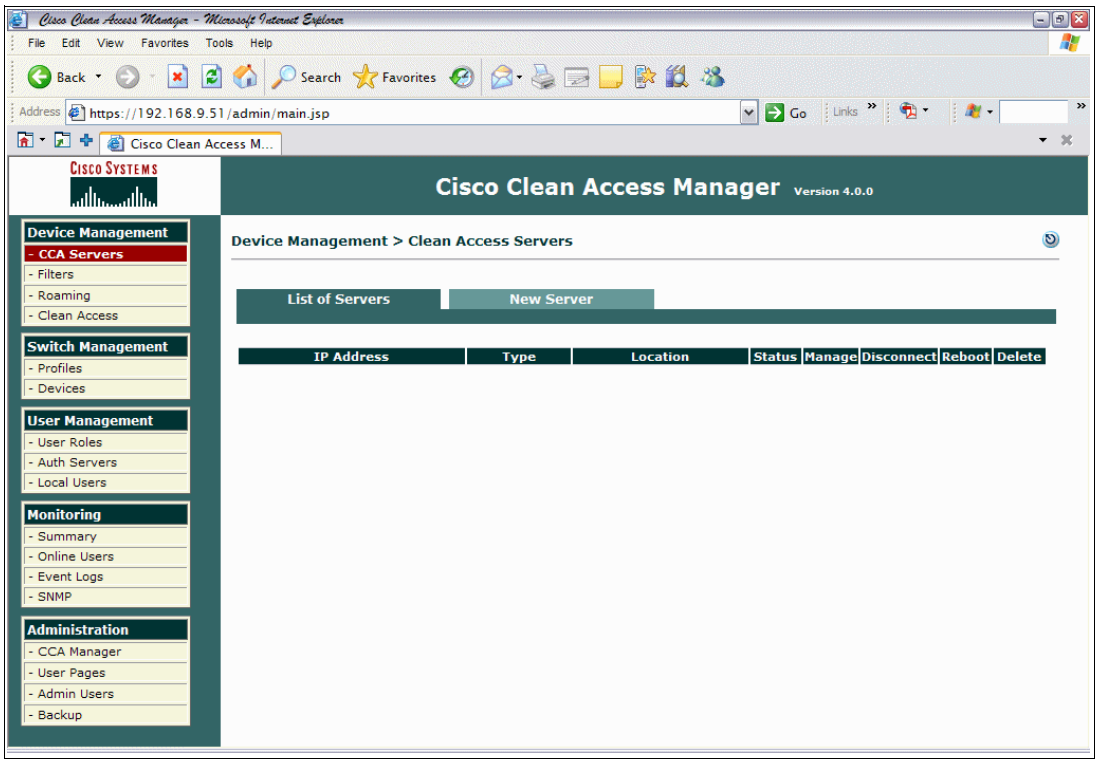


Figure 7-77 Device Management

Downloaded from www.Manualslib.com manuals search engine

5. Select **New Server**. Add the server IP address and server location, and from the drop-down list, select **Out-Of-Band Virtual Gateway** (Figure 7-78).

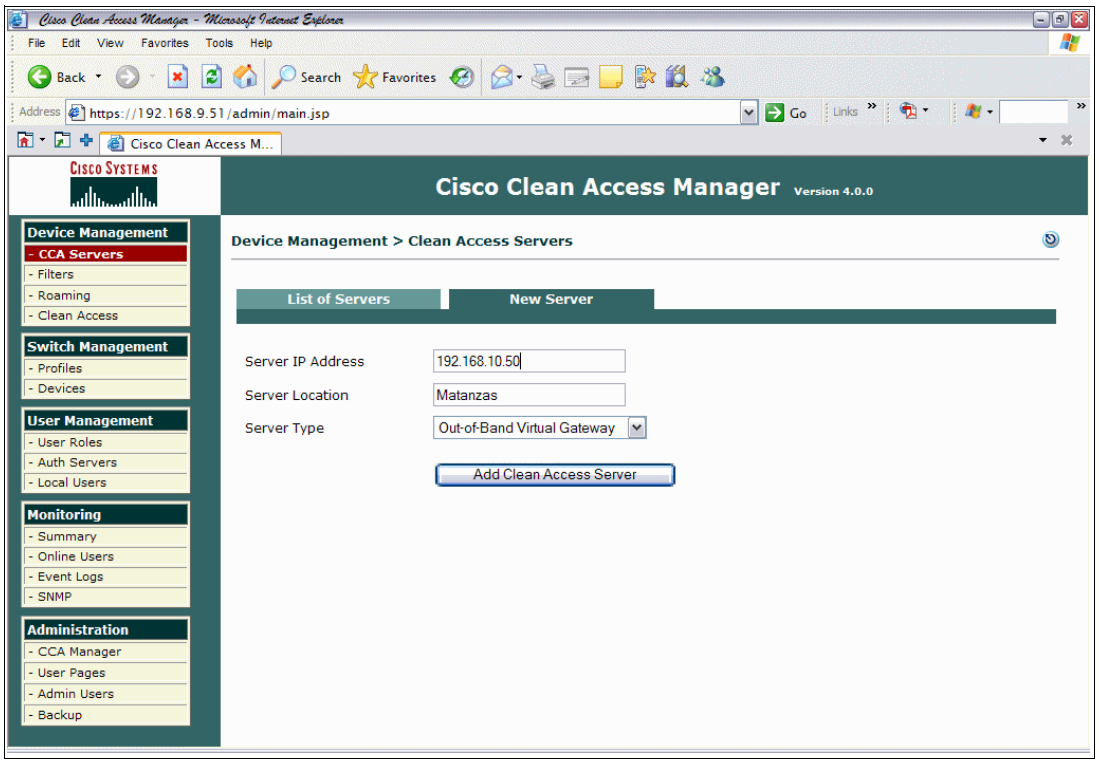


Figure 7-78 Adding a new CAS

6. Click **Add Clean Access Server**.

Downloaded from www.Manualslib.com manuals search engine

7. The CAS should now be visible under **List of Servers**, shown in Figure 7-79.

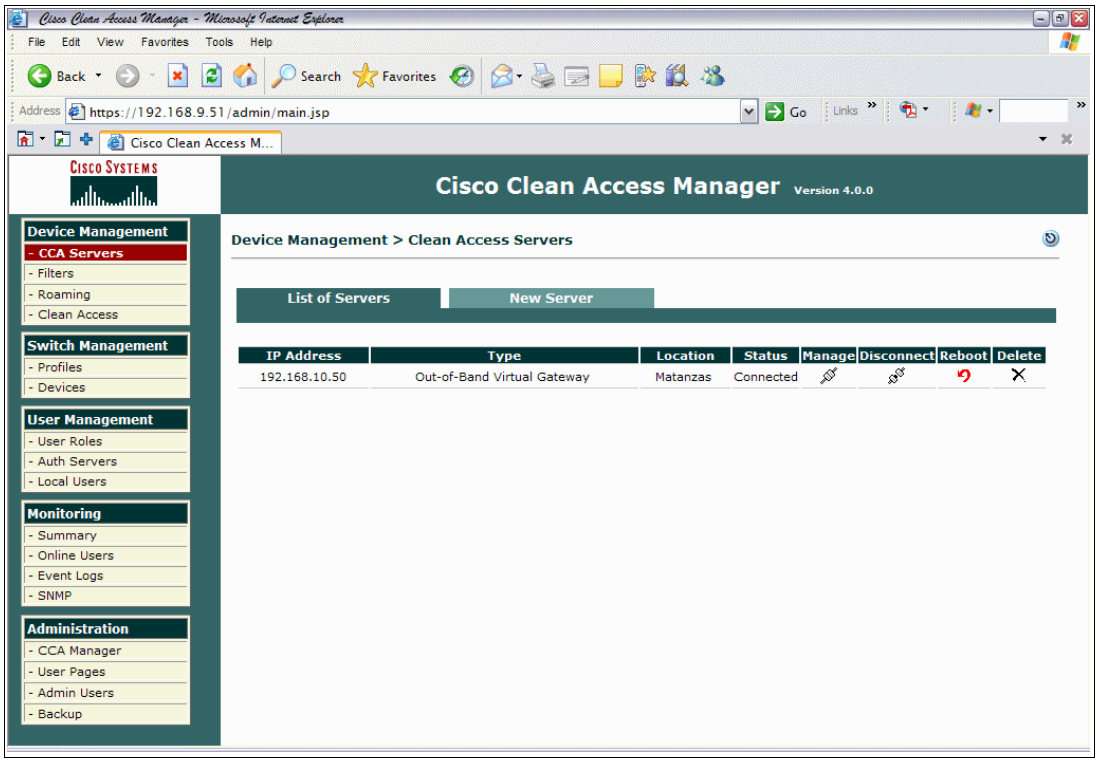


Figure 7-79 Successful CAS addition

Note: If you intend to configure the CAS in Virtual Gateway Mode (in-band or out-of-band), you must leave the untrusted interface (eth1) disconnected until after you have added the CAS to the CAM and completed the VLAN mappings. Keeping eth1 connected while performing initial installation and configuration of the CAS for Virtual Gateway mode will result in network connectivity issues. These will be seen as a native VLAN mismatch on the switch.

Downloaded from www.Manualslib.com manuals search engine

8. Click the Manage icon for the CAS just added. This takes you to the dialog shown in Figure 7-80.

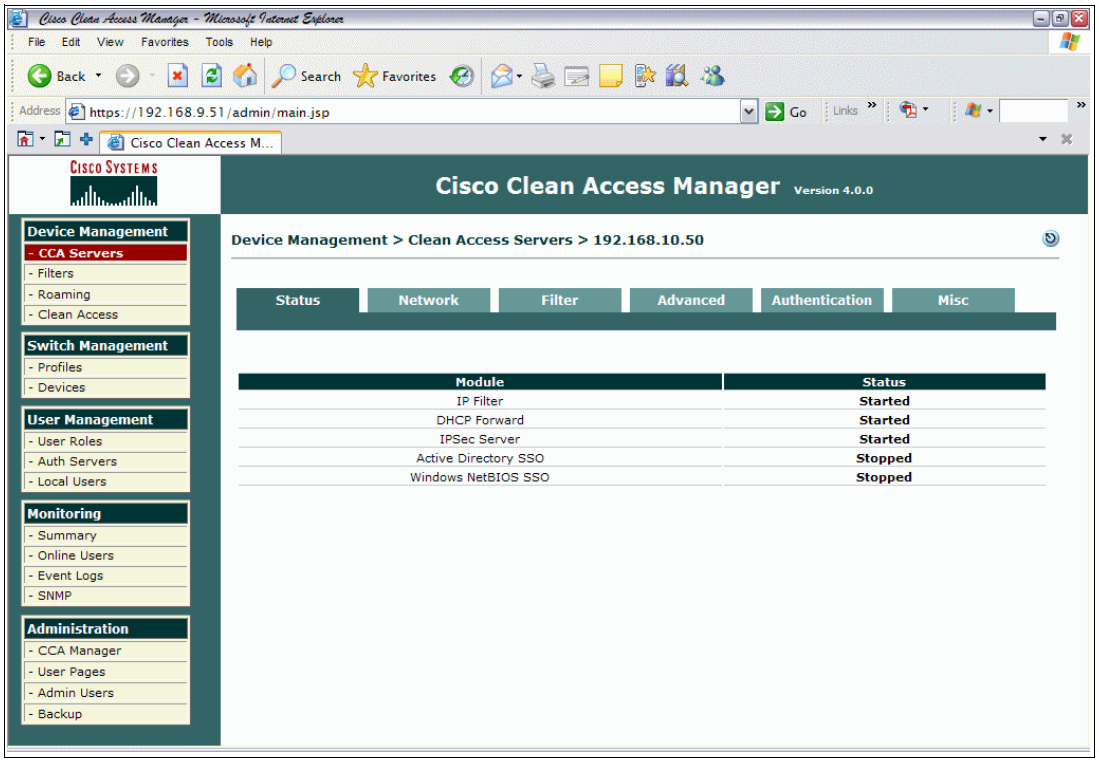


Figure 7-80 CAS Status screen

Downloaded from www.Manualslib.com manuals search engine

9. Select **Device Management** → **CCA Servers** → **Network**. Check that your screen resembles Figure 7-81.

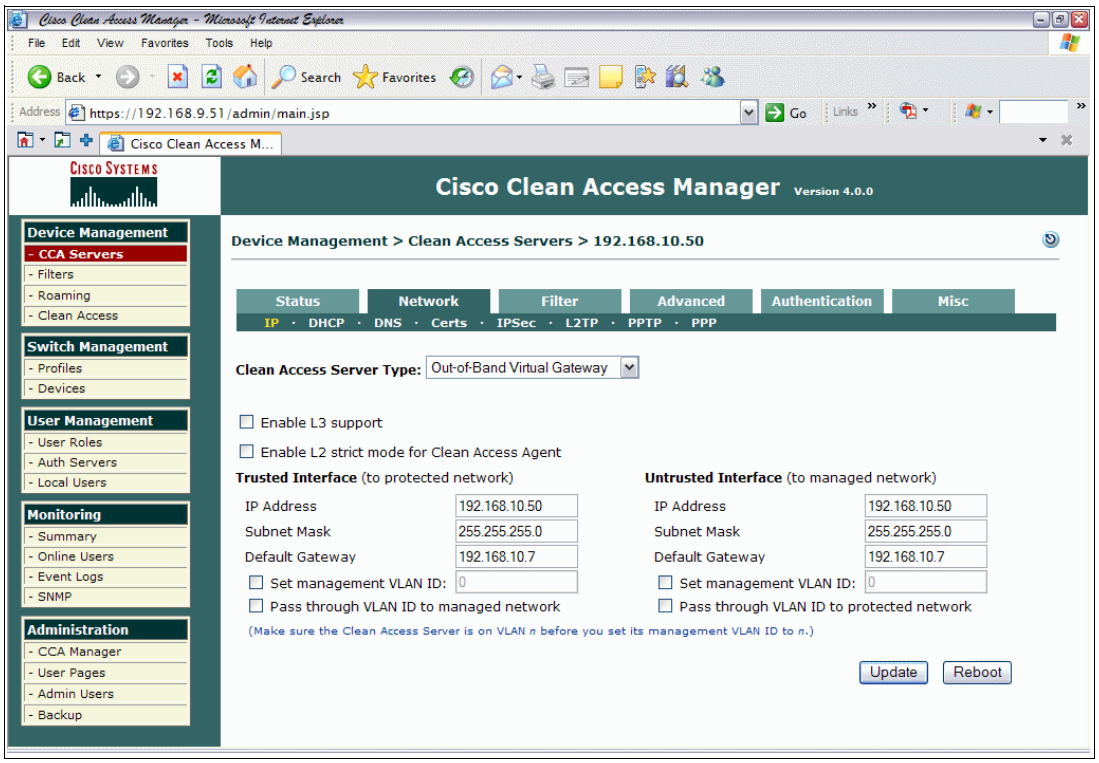

Cisco Clean Access Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.9.51/admin/main.jsp
Go Links
Cisco Clean Access M...
Cisco Systems
Cisco Clean Access Manager Version 4.0.0
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Device Management > Clean Access Servers > 192.168.10.50
Status Network Filter Advanced Authentication Misc
IP · DHCP · DNS · Certs · IPSec · L2TP · PPTP · PPP
Clean Access Server Type: Out-of-Band Virtual Gateway
Enable L3 support
Enable L2 strict mode for Clean Access Agent
Trusted Interface (to protected network)
IP Address 192.168.10.50
Subnet Mask 255.255.255.0
Default Gateway 192.168.10.7
Set management VLAN ID: 0
Pass through VLAN ID to managed network
Untrusted Interface (to managed network)
IP Address 192.168.10.50
Subnet Mask 255.255.255.0
Default Gateway 192.168.10.7
Set management VLAN ID: 0
Pass through VLAN ID to protected network
(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)
Update Reboot

Figure 7-81 Network IP screen

10. Select **Device Management** → **CCA Servers** → **Advanced** → **Managed Subnet**.

11. Enter IP addresses from the *trusted* and *non-trusted networks* (access and authentication VLANs) in the IP Address field. These IP addresses should be static, outside of the DHCP scope, and be neither the network number nor broadcast address of the managed VLAN (for example, 192.168.120.0 or 192.168.120.255). The arbitrary values, VLAN 120 — 192.168.120.50 and VLAN 20 — 192.168.20.50, for each managed subnet are used for our example. Include the appropriate subnet masks and VLAN IDs of the trusted

Downloaded from www.Manualslib.com manuals search engine

and non-trusted networks. The *main subnet* is added by default. For each managed network include the *IP Address* and *subnet mask VLAN ID*, as shown in Figure 7-82. Click **Add Managed Subnet**.

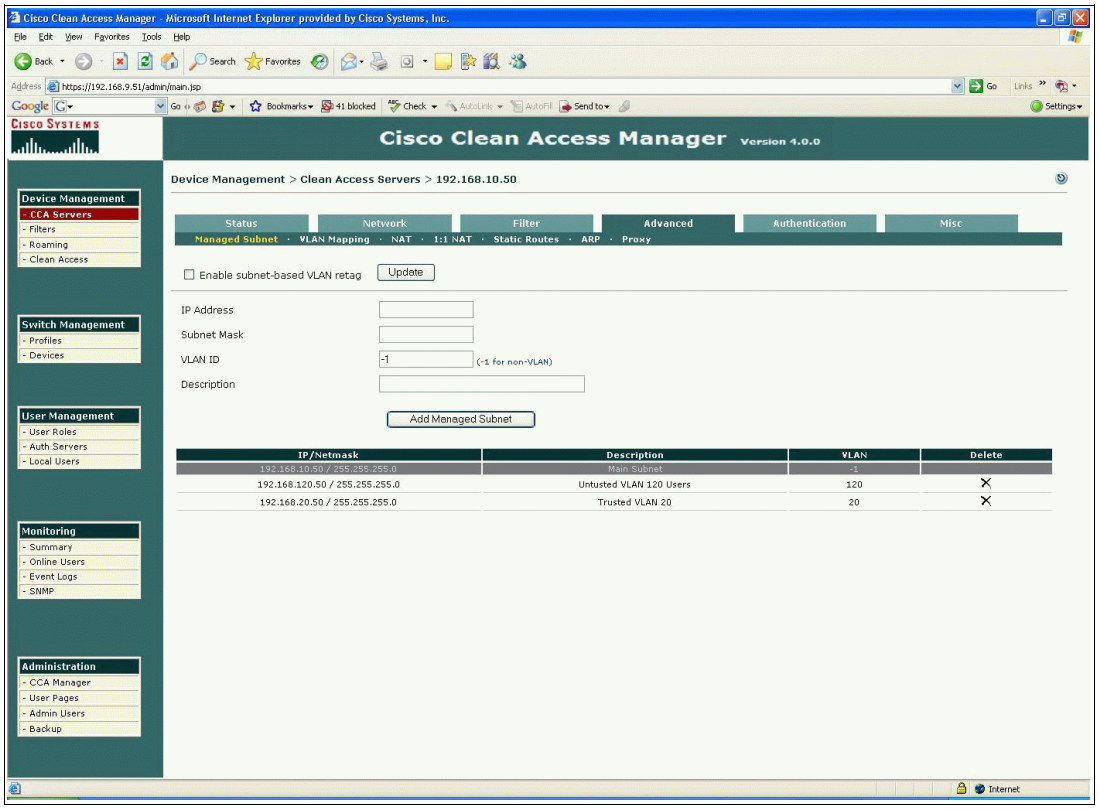


Figure 7-82 Managed subnets

12. Select **Advanced** → **VLAN Mapping**.
13. Check the **Enable VLAN Mapping** box. Click **Update**. The screen will refresh and stay the same. Enter the VLAN ID for the untrusted network VLAN and the VLAN ID for the trusted network VLAN. Add a description if desired.

Downloaded from www.Manualslib.com manuals search engine

14. Click **Add Mapping**. Confirmation of the successful mapping will appear (Figure 7-83).

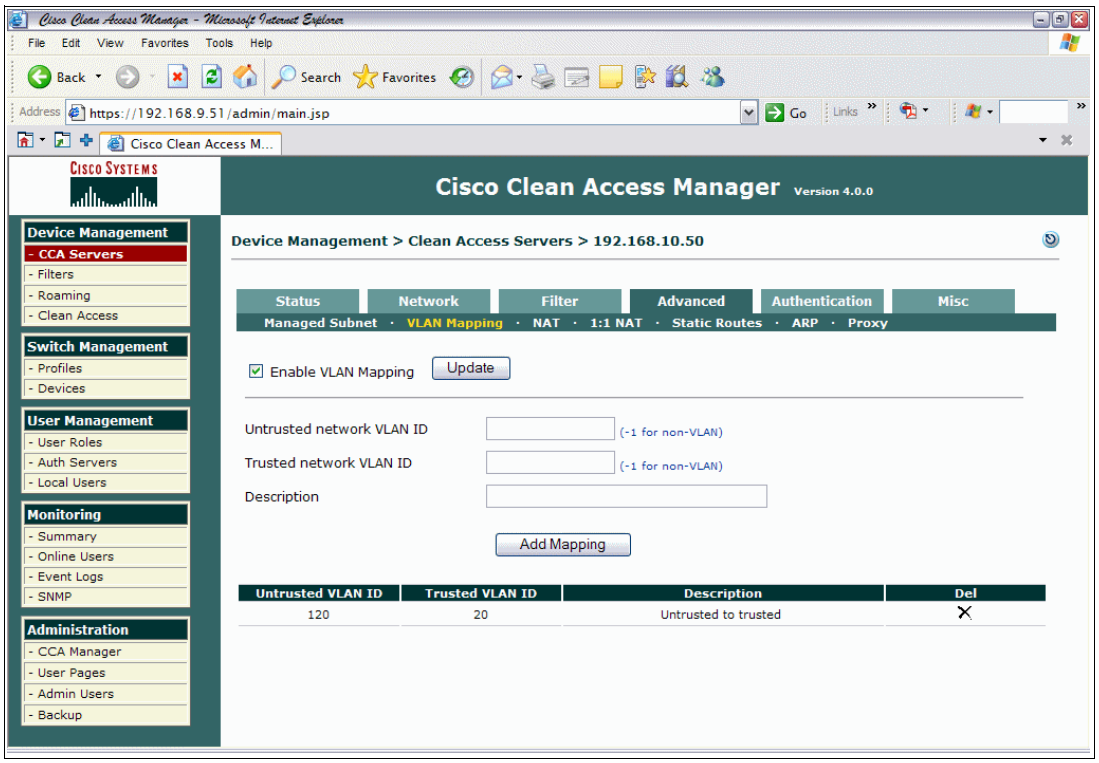


Figure 7-83 VLAN mapping example

> **Note:** In our example, the client's port is initially set to VLAN 20. By using VLAN mapping, the client will receive a VLAN 20 (access VLAN) IP address from DHCP. Should the client not be compliant, the CAM will change the port's VLAN membership via SNMP to VLAN120 (Auth VLAN). This will force all traffic from the client through the CAS. Once the CAS informs the CAM that the client is *healthy*, the CAM will again change the client's port VLAN membership back to VLAN 20 via SNMP. The client will then access the network directly through the switch, bypassing the CAS.

Configure default login page

To configure the default login page follow these steps:

1. Click **Administration** → **User Pages** → **Login Page**.

Downloaded from www.Manualslib.com manuals search engine

2. Click **Add**. The VLAN ID should be an asterisk (*), the subnet information should be ‘*’/’*’ and the operating system should be set to *ALL*. This will allow Web login and Clean Access Agent users to authenticate (Figure 7-84).

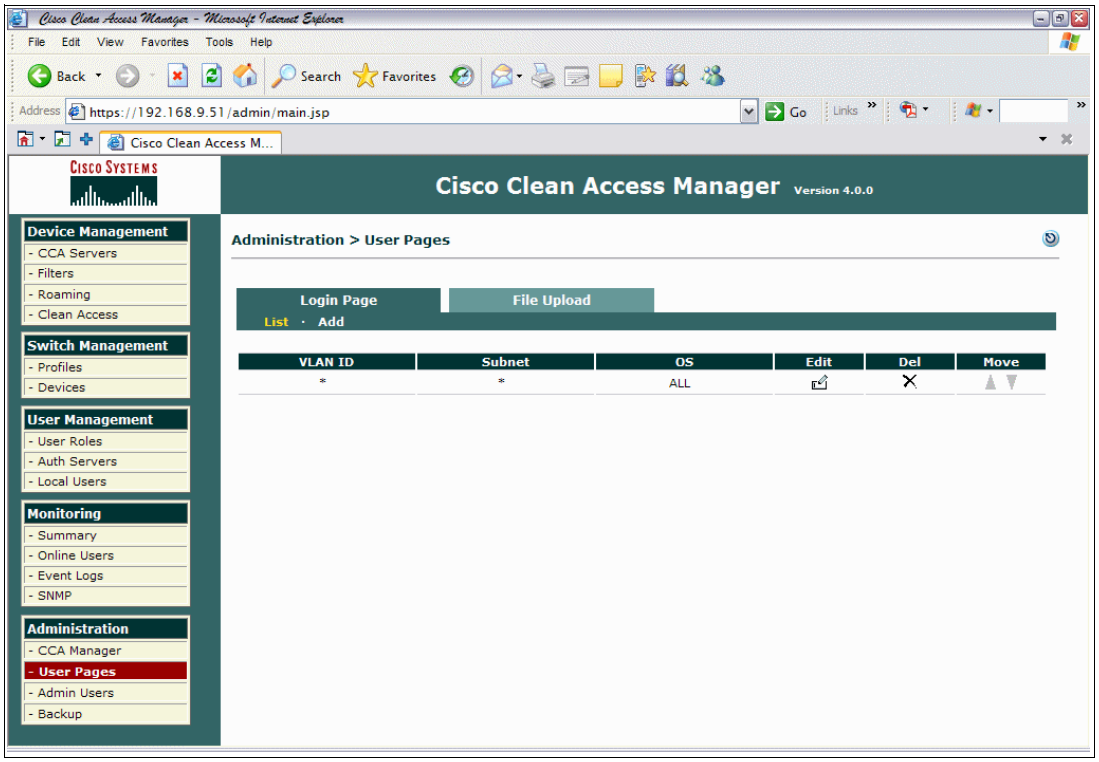


Figure 7-84 Login page

Configuring a Switch Group

To configure a switch group follow these steps.

1. Select **Switch Management** → **Profiles** → **Group** → **New**.

Downloaded from www.Manualslib.com manuals search engine

2. Enter the group name and description (Figure 7-85).

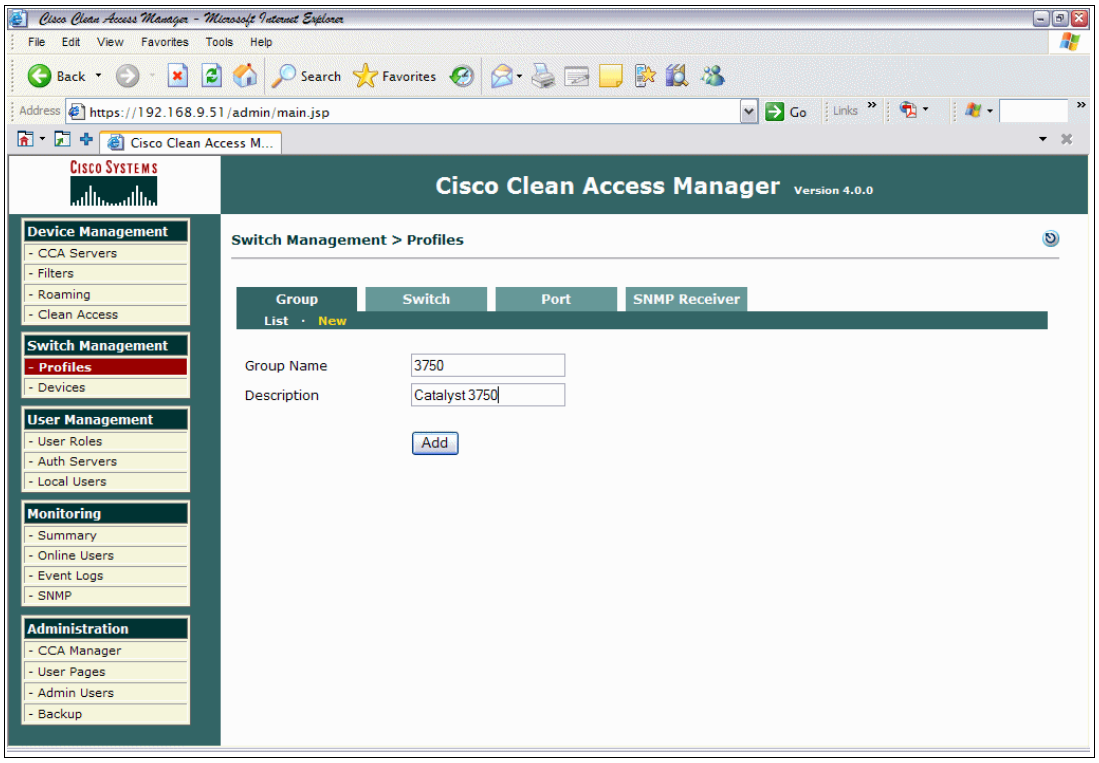


Figure 7-85 Switch Group creation

3. Click **Add**.

Downloaded from www.Manualslib.com manuals search engine

4. Verify your new switch group (Figure 7-86).

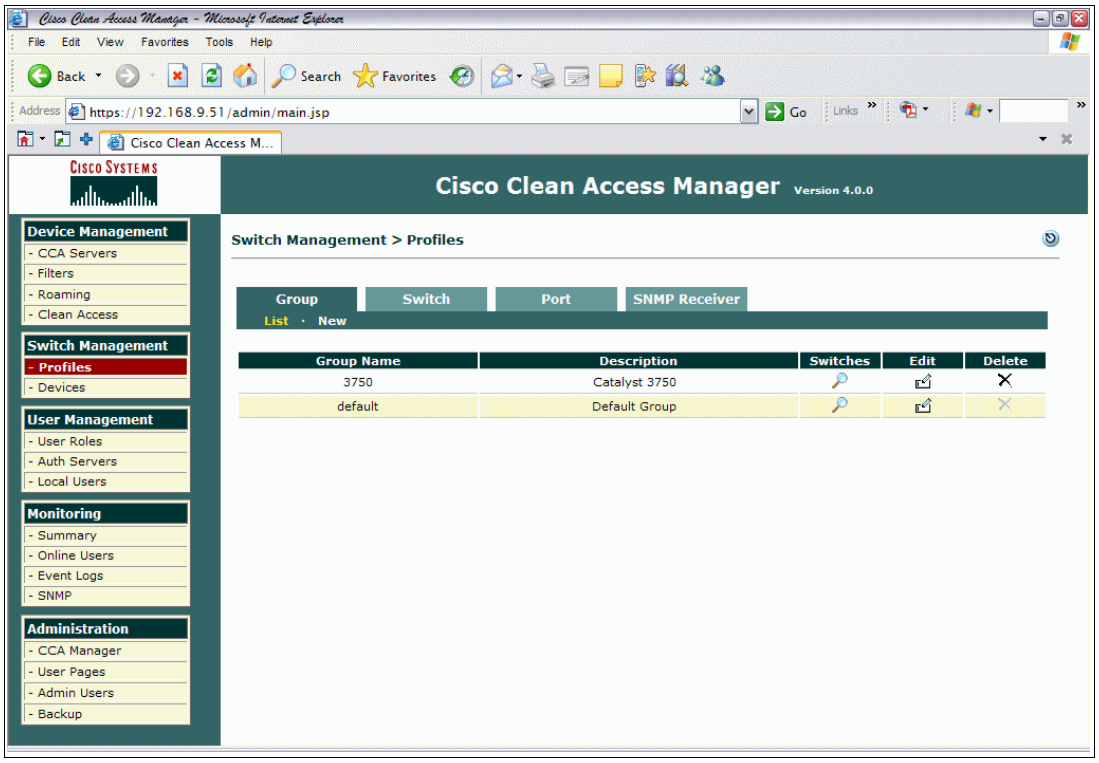


Figure 7-86 Switch Group verification

Downloaded from www.Manualslib.com manuals search engine

Configuring a switch profile

To configure a switch profile follow these steps:

1. From *Switch Management* in the main menu, select **Profiles** → **Switch** → **New** (Figure 7-87).

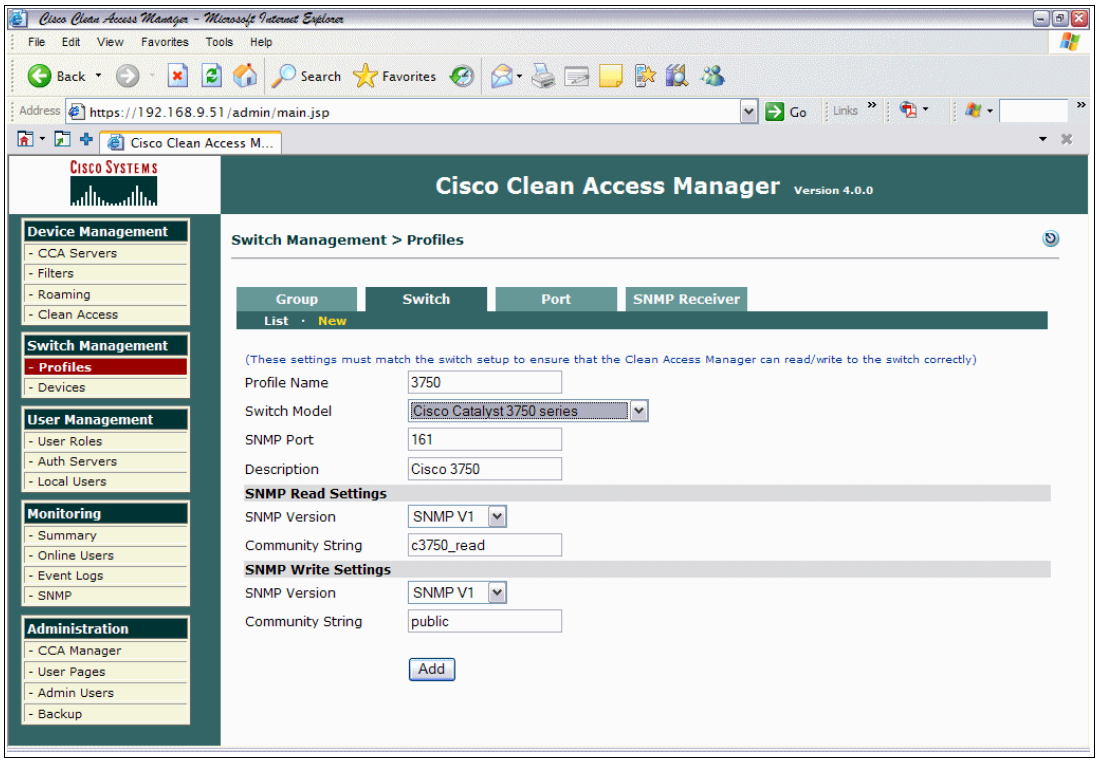


Figure 7-87 New switch profile

2. Fill in the fields as appropriate. In our scenario we used:

Profile Name	3750
Switch Model	Cisco Catalyst 3750 series
SNMP Port	161
Description	Cisco 3750
SNMP Read Settings	SNMP Version 1
SNMP Read Settings	Community String c3750_read
SNMP Write Settings	SNMP Version 1
SNMP Write Settings	public

Downloaded from www.Manualslib.com manuals search engine

3. Click **Add**. A confirmation of the new profile will appear, as shown in Figure 7-88.

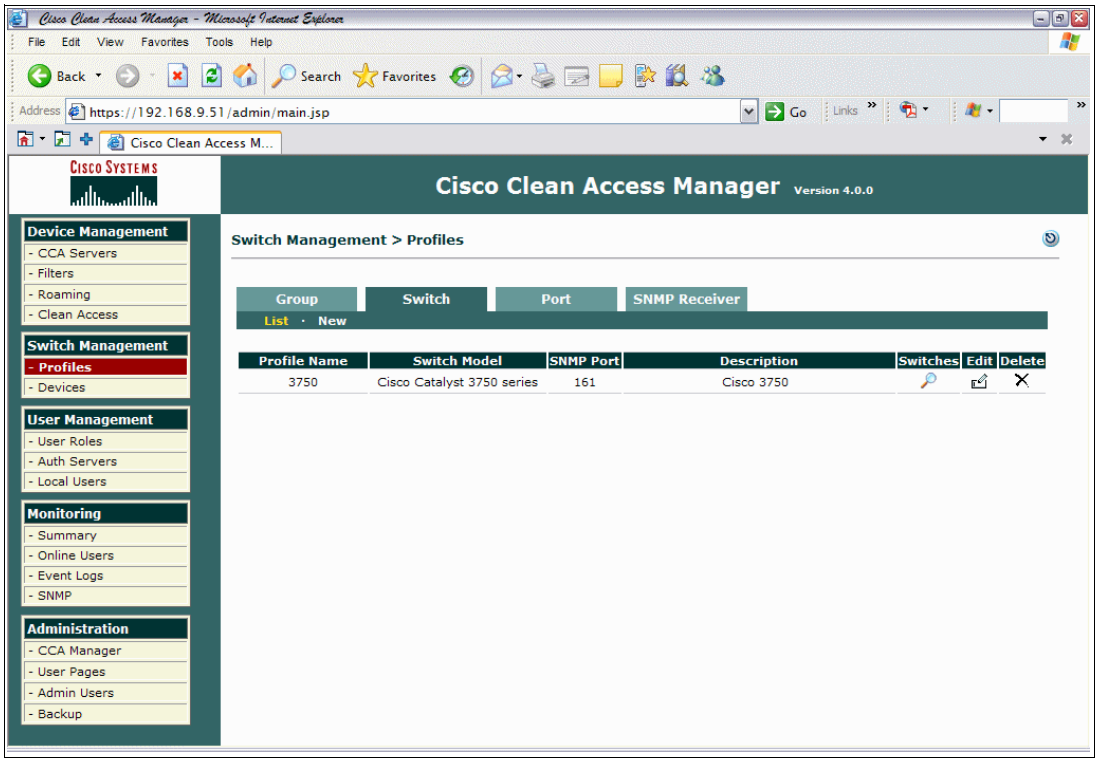


Figure 7-88 Switch profile

Configuring Port Profile

There are three types of port profiles for switch ports: uncontrolled, controlled, and controlled using role settings.

- Switch ports should use *uncontrolled* port profiles.
- Clients connections should use *controlled* port profiles.

Downloaded from www.Manualslib.com manuals search engine

When a client connects to a controlled port, the port is assigned to the authentication VLAN. After the client has been successfully authenticated, the port is assigned to the Access VLAN specified in the port profile or the role settings.

1. Select **Switch Management** → **Profiles** → **Port** → **New** (Figure 7-89).

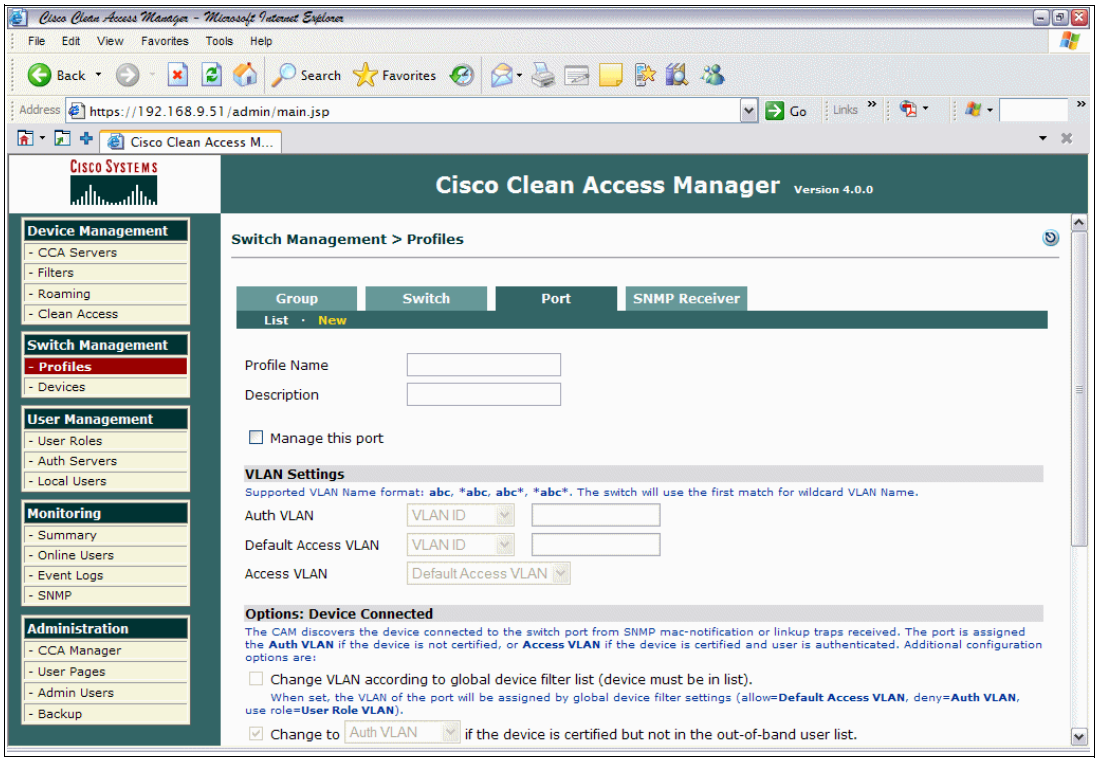

Cisco Clean Access Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.9.51/admin/main.jsp
Go Links
Cisco Clean Access M...
Cisco Systems
Cisco Clean Access Manager Version 4.0.0
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Switch Management > Profiles
Group Switch Port SNMP Receiver
List · New
Profile Name
Description
Manage this port
VLAN Settings
Supported VLAN Name format: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name.
Auth VLAN VLAN ID
Default Access VLAN VLAN ID
Access VLAN Default Access VLAN
Options: Device Connected
The CAM discovers the device connected to the switch port from SNMP mac-notification or linkup traps received. The port is assigned the Auth VLAN if the device is not certified, or Access VLAN if the device is certified and user is authenticated. Additional configuration options are:
Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (allow=Default Access VLAN, deny=Auth VLAN, use role=User Role VLAN).
Change to Auth VLAN if the device is certified but not in the out-of-band user list.

Figure 7-89 New port profile

2. Enter a profile name. We used `Control_20`. Enter a description. Ensure that **Manage this port** is checked.
3. Under VLAN Settings, set the Auth VLAN ID to 120. Set the Default Access VLAN ID to 20. Access VLAN should be set to Default Access VLAN.

Downloaded from www.Manualslib.com manuals search engine

4. Under Options: Device Disconnect, check the box **Remove out-of-band online user when SNMP link-down is received** (Figure 7-90).

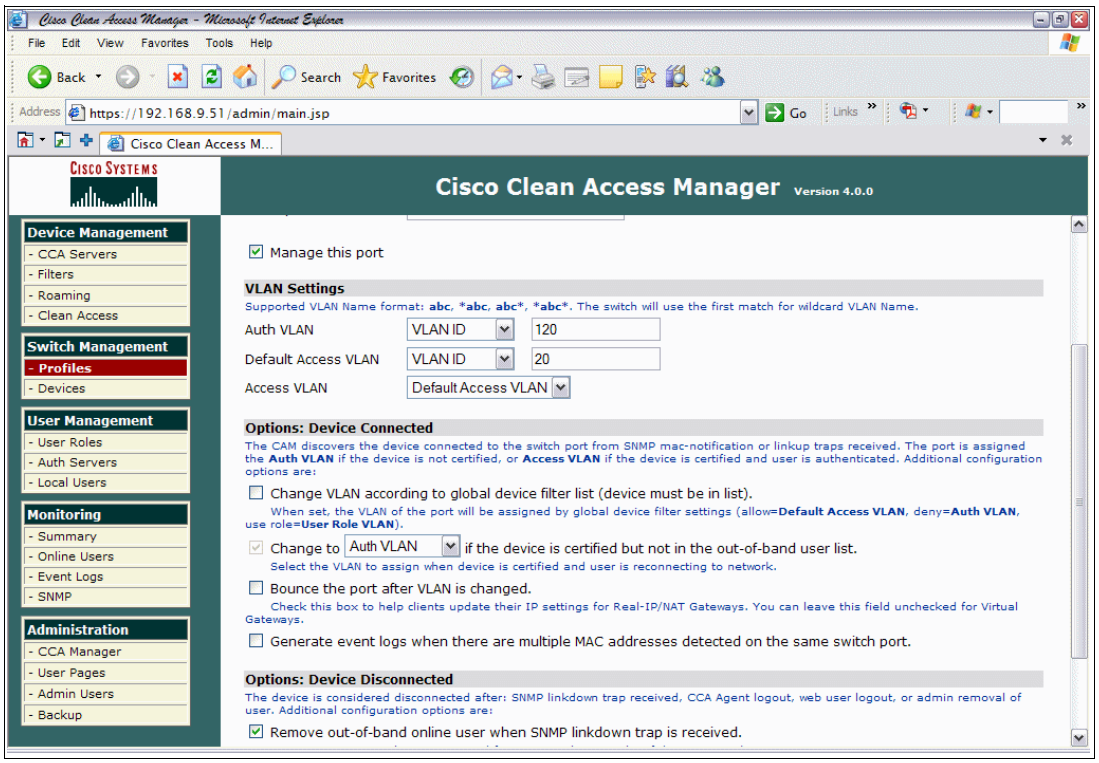

Cisco Clean Access Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.9.51/admin/main.jsp
Go Links
Cisco Clean Access M...
Cisco Systems
Cisco Clean Access Manager Version 4.0.0
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Manage this port
VLAN Settings
Supported VLAN Name format: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name.
Auth VLAN VLAN ID 120
Default Access VLAN VLAN ID 20
Access VLAN Default Access VLAN
Options: Device Connected
The CAM discovers the device connected to the switch port from SNMP mac-notification or linkup traps received. The port is assigned the Auth VLAN if the device is not certified, or Access VLAN if the device is certified and user is authenticated. Additional configuration options are:
Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (allow=Default Access VLAN, deny=Auth VLAN, use role=User Role VLAN).
Change to Auth VLAN if the device is certified but not in the out-of-band user list.
Select the VLAN to assign when device is certified and user is reconnecting to network.
Bounce the port after VLAN is changed.
Check this box to help clients update their IP settings for Real-IP/NAT Gateways. You can leave this field unchecked for Virtual Gateways.
Generate event logs when there are multiple MAC addresses detected on the same switch port.
Options: Device Disconnected
The device is considered disconnected after: SNMP linkdown trap received, CCA Agent logout, web user logout, or admin removal of user. Additional configuration options are:
Remove out-of-band online user when SNMP linkdown trap is received.

Figure 7-90 Managed profile creation

Downloaded from www.Manualslib.com manuals search engine

5. Click **Add**. The configured switch profiles will be displayed (Figure 7-91).

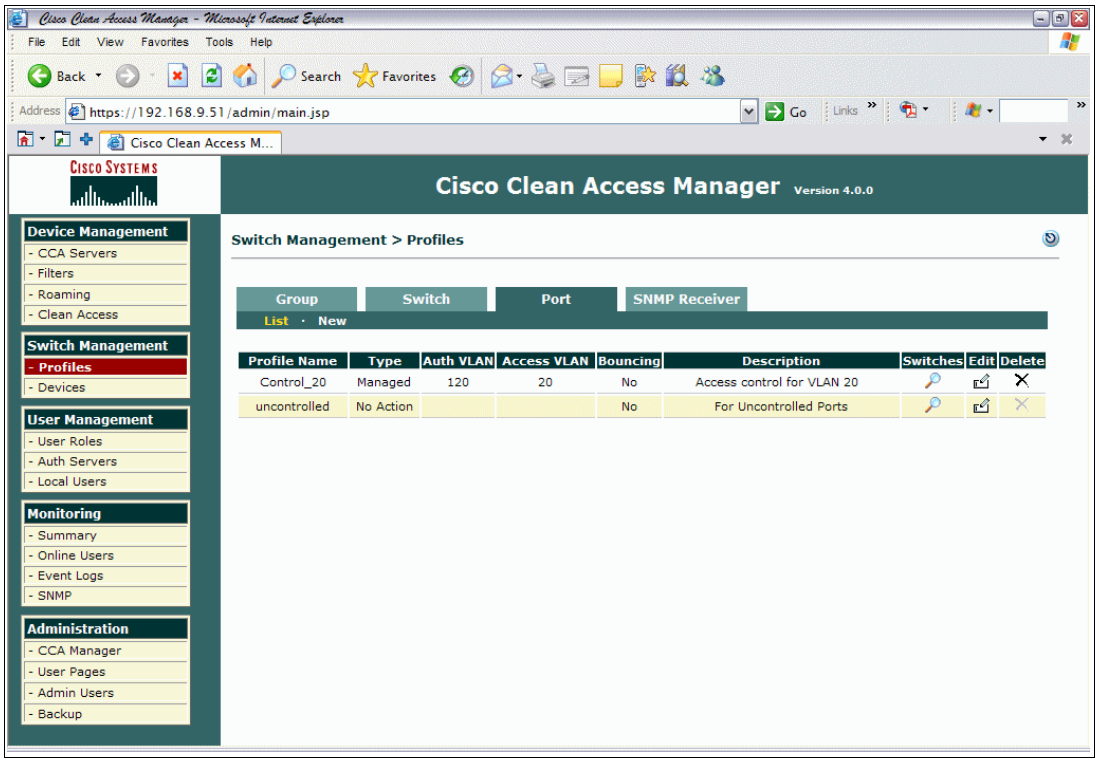


Figure 7-91 Configured switch profiles

Configuring SNMP receiver

SNMP receiver setup provides settings for the SNMP receiver running on the CAM, which receives the mac-notification/link-down SNMP trap notifications from the controlled switches and sets the VLAN value on the corresponding switch ports.

1. Click **Switch Management** → **Profiles** → **SNMP Receiver**.

Downloaded from www.Manualslib.com manuals search engine

2. Complete as necessary, depending on the version of SNMP being used and the SNMP community strings in the environment (Figure 7-92).

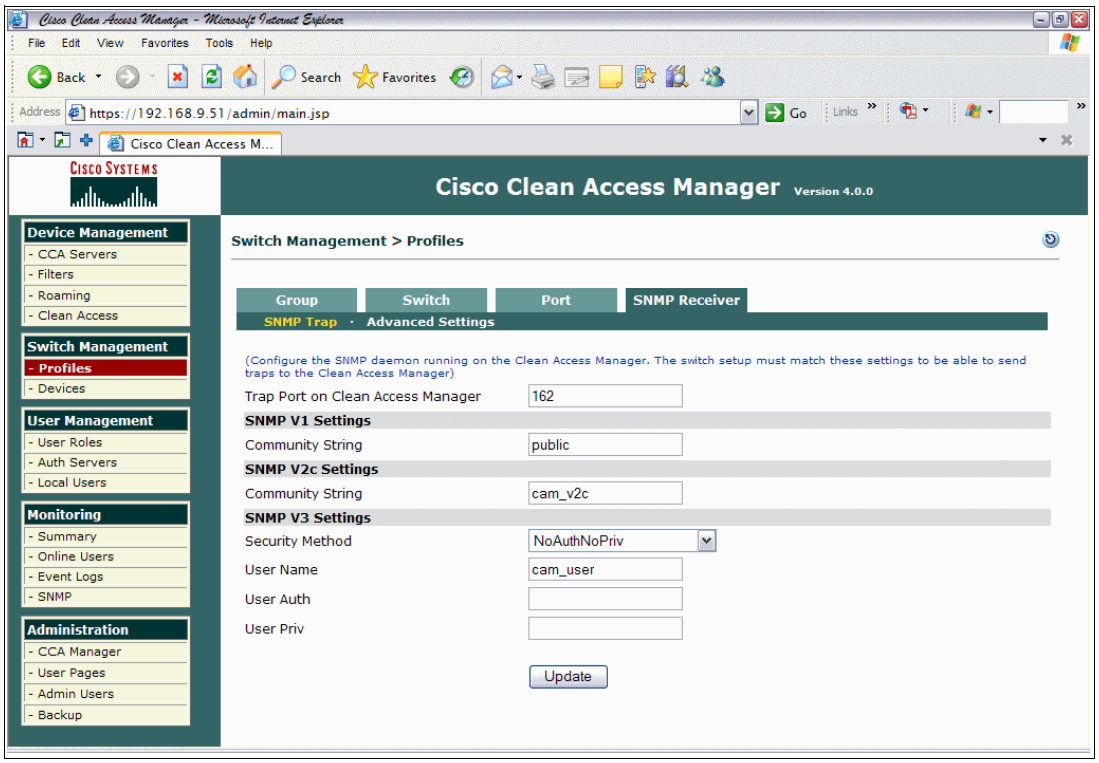


Figure 7-92 SNMP configuration

3. Click **Add**.

> **Note:** Be very wary of the version of SNMP used in the environment. Only SNMPv3 provides any real security, but not all devices may support SNMPv3. Do not use the default community strings, and use access lists on the switches to control which devices can communicate with them using SNMP.

Adding a managed switch

This allows the CAM to discover switches it will manage in the subnets specified. This can be done in two ways, either by entering the exact IP address of the switch if already known, or by searching a specific subnet. In our example, we are specifying the exact IP address of the switch.

1. Select **Switch Management** → **Devices** → **Switches** → **New**.
2. **3750** should be selected from the Switch Profile drop-down list, Switch Group should be left as default, Default Port Profile should be left as uncontrolled,

Downloaded from www.Manualslib.com manuals search engine

the IP address of the switch should be entered in t**he *IP Address* b**ox, and a description entered in the Description field (Figure 7-93).

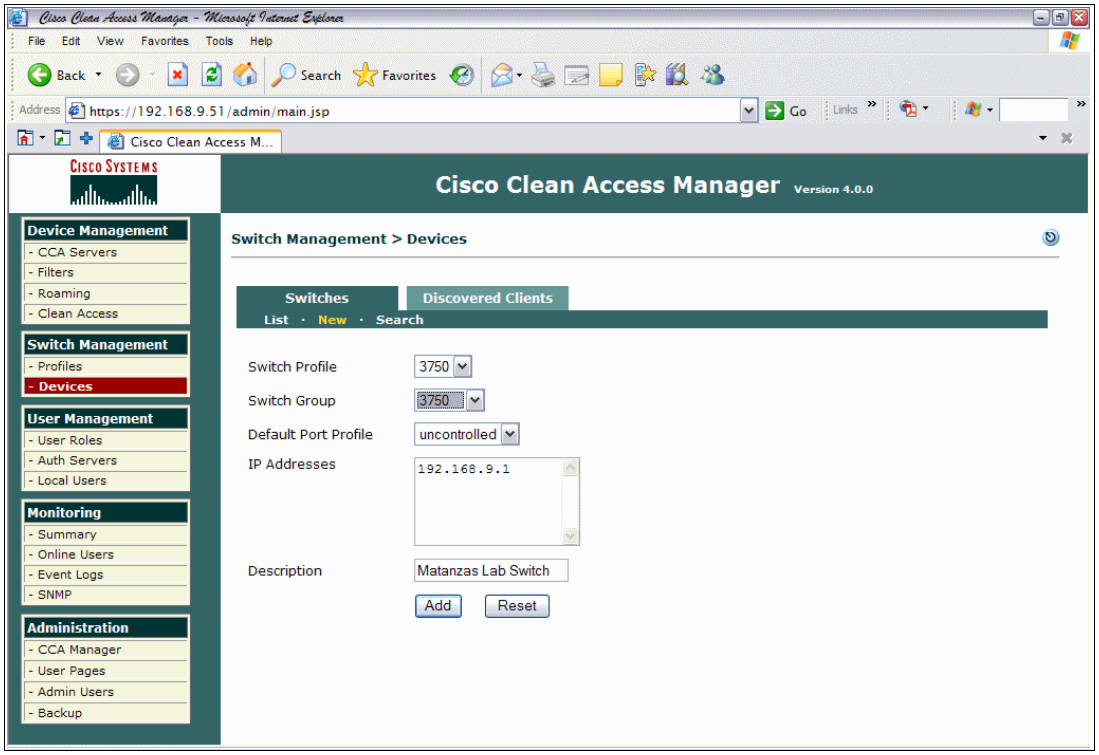


Figure 7-93 Manually adding a switch to be managed

3. Click **Add**.
4. The switch can been seen by selecting **Switch Management** → **Devices** → **List**.

Downloaded from www.Manualslib.com manuals search engine

5. As seen in Figure 7-94, click the Ports icon.

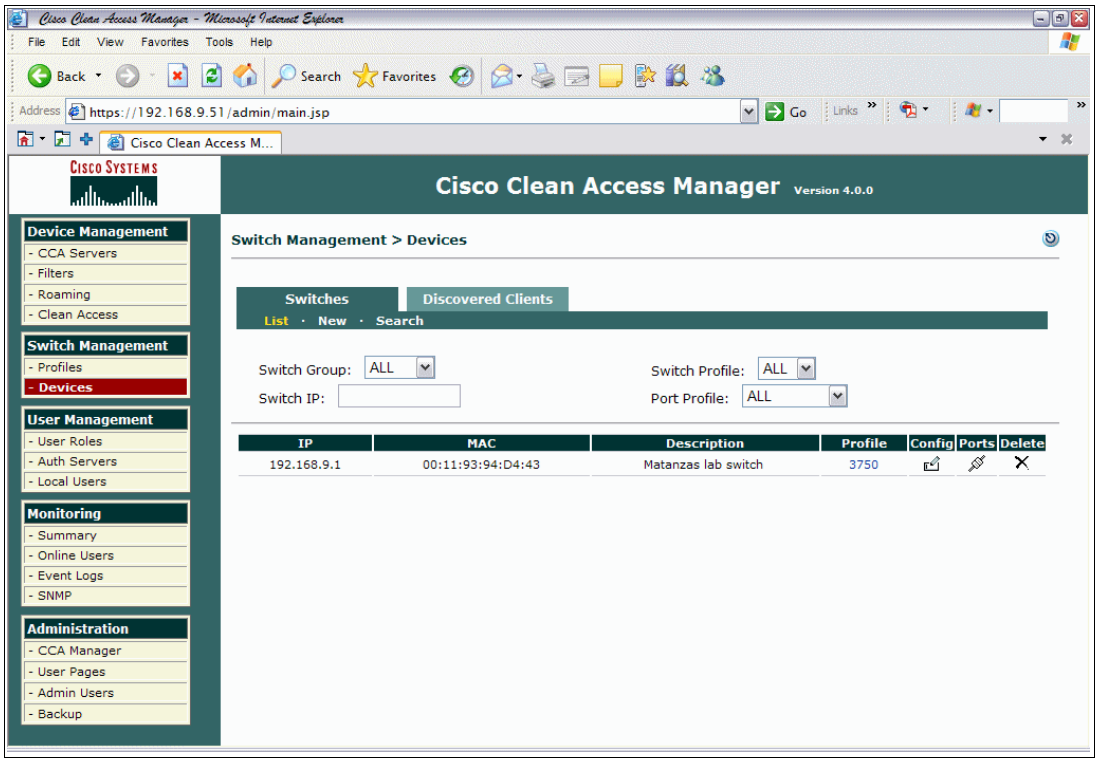


Figure 7-94 Managed switch

Downloaded from www.Manualslib.com manuals search engine

6. Under Profile, use the drop-down list to configure the ports as appropriate. Our client was installed on port fa1/0/12, (Figure 7-95) so the profile was set to Control_20.

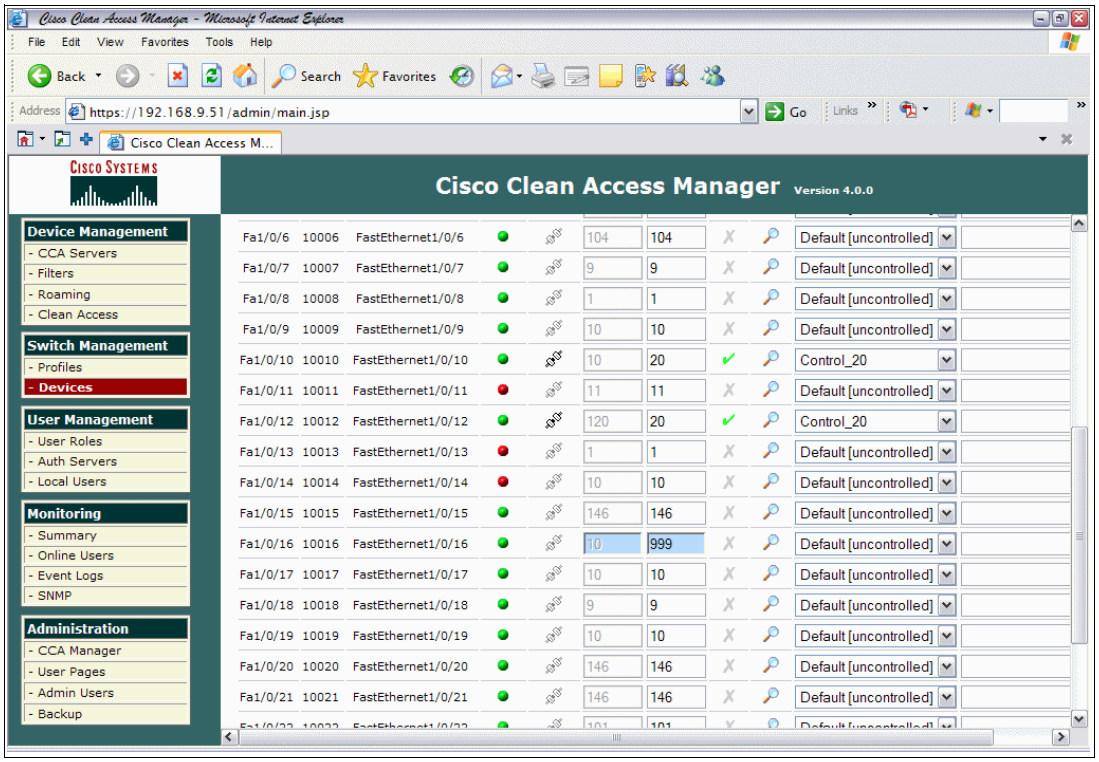

Cisco Clean Access Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.9.51/admin/main.jsp
Go Links
Cisco Clean Access M...
Cisco Systems
Cisco Clean Access Manager Version 4.0.0
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Fa1/0/6 10006 FastEthernet1/0/6 104 104 Default [uncontrolled]
Fa1/0/7 10007 FastEthernet1/0/7 9 9 Default [uncontrolled]
Fa1/0/8 10008 FastEthernet1/0/8 1 1 Default [uncontrolled]
Fa1/0/9 10009 FastEthernet1/0/9 10 10 Default [uncontrolled]
Fa1/0/10 10010 FastEthernet1/0/10 10 20 Control_20
Fa1/0/11 10011 FastEthernet1/0/11 11 11 Default [uncontrolled]
Fa1/0/12 10012 FastEthernet1/0/12 120 20 Control_20
Fa1/0/13 10013 FastEthernet1/0/13 1 1 Default [uncontrolled]
Fa1/0/14 10014 FastEthernet1/0/14 10 10 Default [uncontrolled]
Fa1/0/15 10015 FastEthernet1/0/15 146 146 Default [uncontrolled]
Fa1/0/16 10016 FastEthernet1/0/16 10 999 Default [uncontrolled]
Fa1/0/17 10017 FastEthernet1/0/17 10 10 Default [uncontrolled]
Fa1/0/18 10018 FastEthernet1/0/18 9 9 Default [uncontrolled]
Fa1/0/19 10019 FastEthernet1/0/19 10 10 Default [uncontrolled]
Fa1/0/20 10020 FastEthernet1/0/20 146 146 Default [uncontrolled]
Fa1/0/21 10021 FastEthernet1/0/21 146 146 Default [uncontrolled]

Figure 7-95 Applying profiles to ports. Note port fa1/0/12

> **Note:** An audit of what is attached to each switchport should be conducted before setting the profile. It is likely that clientless devices (such as printers, faxes, IP phones, and so on) will have a different profile from an end-user workstation, and different user groups may need different profiles applied.

Defining user roles

User roles must be defined to classify the user for the duration of their session. This classification of the user controls traffic policies, bandwidth restrictions, session duration, and VLAN assignment.

1. Click **User Management** → **User Roles** → **New Roles**.

Downloaded from www.Manualslib.com manuals search engine

2. Add the role name and role description as appropriate. Our example uses the name *AllowAll*. Select the options as appropriate. The fields of main importance here are Role Type and Out-Of-Band User Role VLAN. For our example, we used *Normal Login Role* and *VLAN ID 20*, respectively (Figure 7-96).

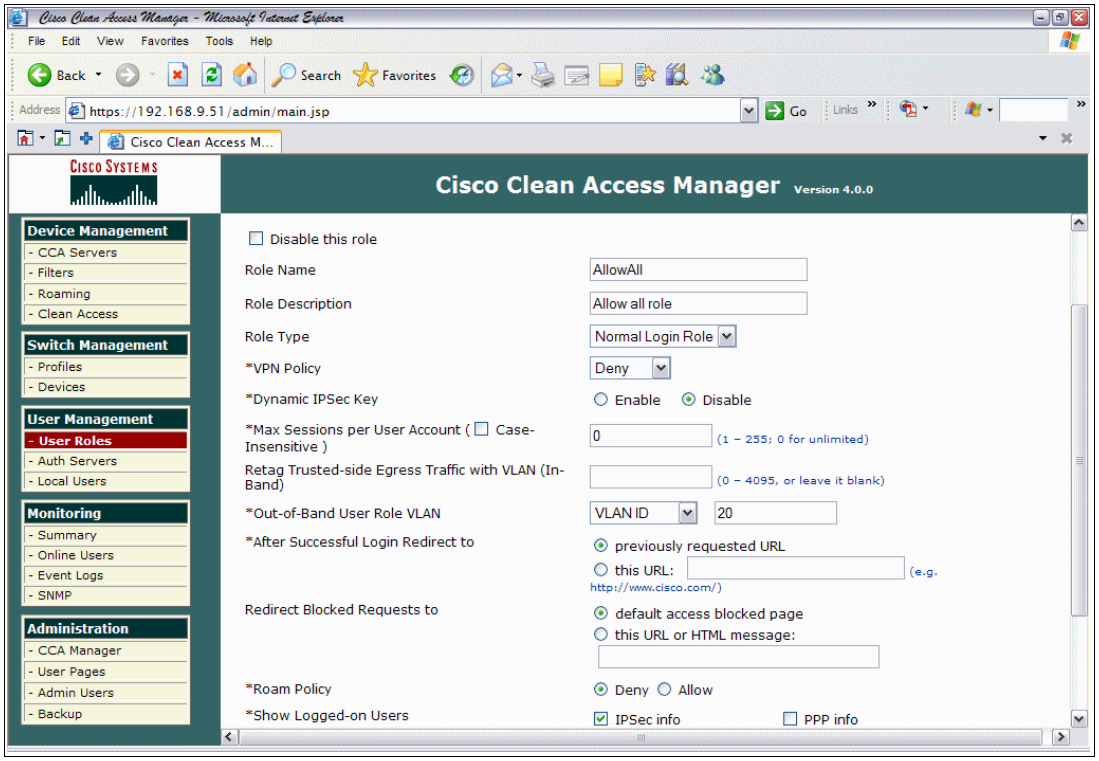


Figure 7-96 Defining a user role

3. Click **Save Role** when completed.

Downloaded from www.Manualslib.com manuals search engine

4. The new role should be visible under *List Of Roles*, depicted in Figure 7-97.

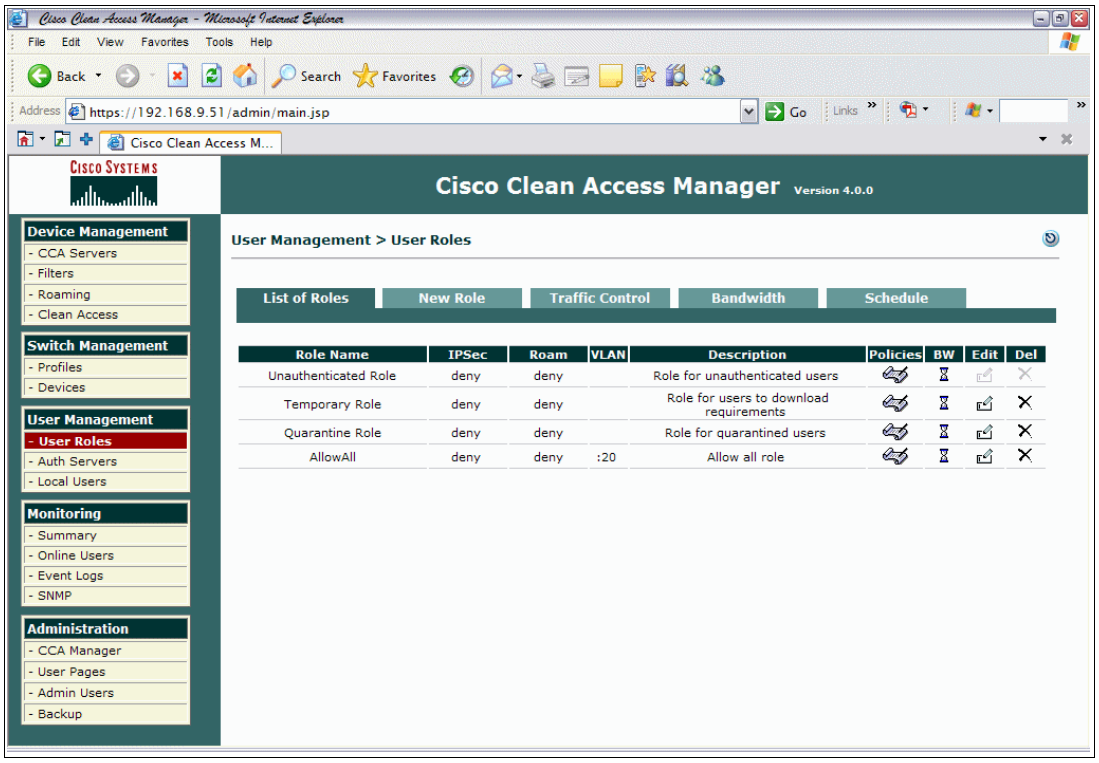


Figure 7-97 List of Roles

Creating traffic policies

For new installations of Cisco NAC Appliance, the default allows all traffic from the trusted network to the untrusted network, and to block all traffic from the untrusted network to the trusted network.

Two types of traffic policies are available, IP-based policies and host-based policies:

IP-based policies Allow you to specify IP protocol numbers, as well as source and destination port numbers. IP-based policies can block or allow traffic moving from the untrusted to the trusted network and vice-versa.

Host-based policies Are less flexible than IP-based policies, but have the advantage of allowing a host to be specified by host name or domain name when a host has multiple or dynamic IP addresses.

1. Click **User Management** → **User Roles** → **Traffic Control** → **IP**.

Downloaded from www.Manualslib.com manuals search engine

2. From the first drop-down menu, select the role you have created. In our example that is *AllowAll*. In the second drop-down menu, select **Trusted** → **Untrusted**. Click **Select** (Figure 7-98).

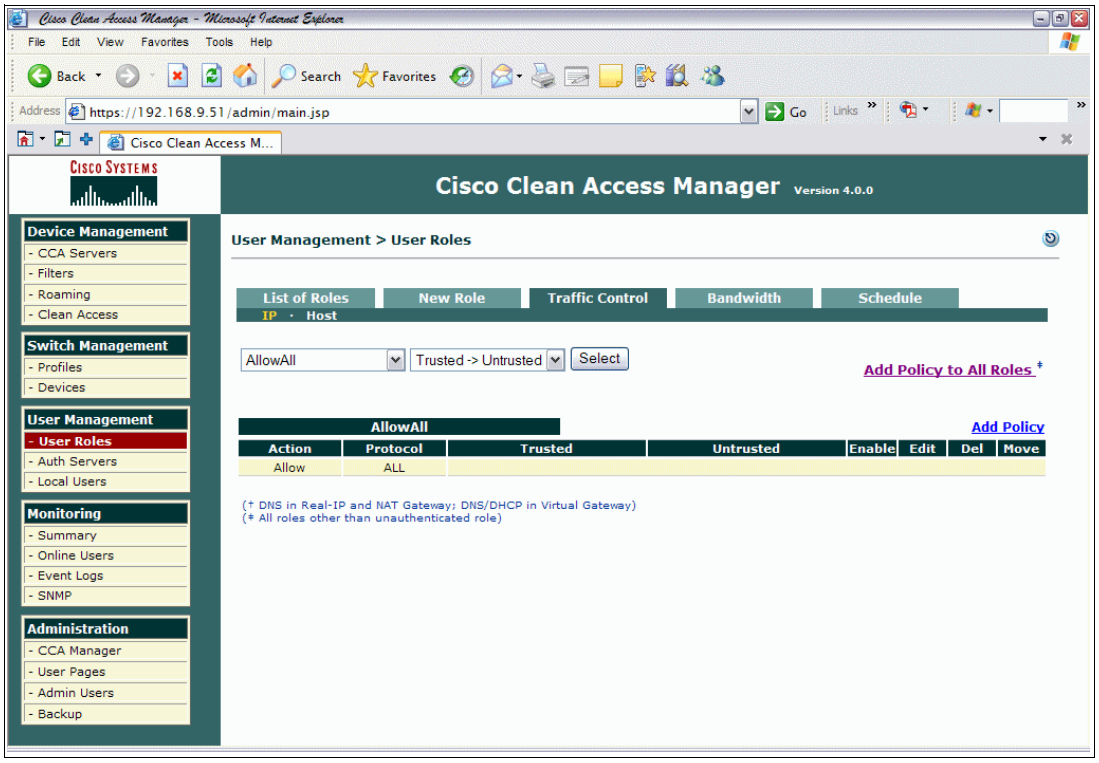


Figure 7-98 Rules for trusted to untrusted

3. The action should be *Allow* and the protocol should be *All*.
4. Repeat step 2, this time selecting **Untrusted** → **Trusted** from the second drop-down menu. Click **Submit**.

Downloaded from www.Manualslib.com manuals search engine

5. The action should be *Allow* and the protocol should be *All* (Figure 7-99).

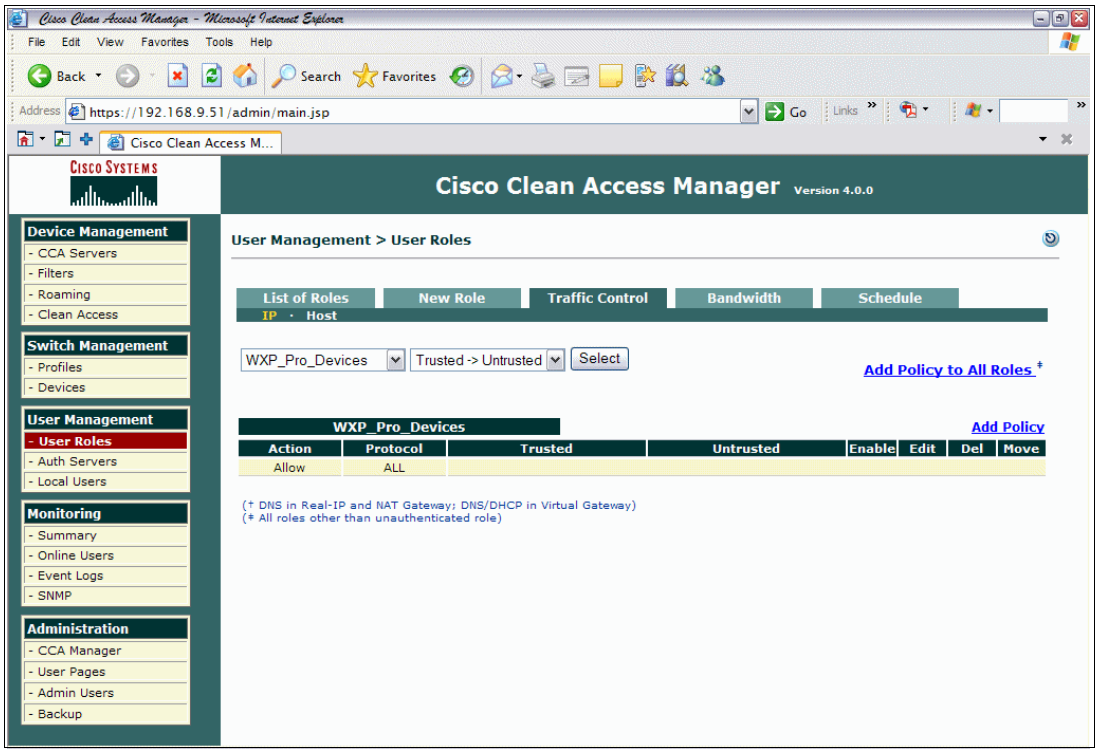


Figure 7-99 Rules for untrusted to trusted

6. Select the group you created (*AllowAll*) from the first drop-down menu. Select **Untrusted** → **Trusted** from the second drop-down menu. Click **Add Policy**.

7. This rule will be to allow access from the Auth VLAN to the Security Compliance Manager. Set the following parameters:

   Action: Allow
   State: Enabled
   Category: IP
   Protocol: TCP
   Untrusted: 192.168.20.0/255.255.255.0:*
   Trusted: 192.168.9.220/255.255.255.255:*
   Description: Allow access to Security Compliance Manager

8. Click **Add Policy**.

9. Repeat step 7, changing *Trusted* to *192.168.104.10* and *Description* to *Allow Access to TCM*.

10. Repeat step 7, changing *Protocol* to *ICMP* and *Type* to *Any* for both the Security Compliance Manager and Tivoli Configuration Manager.

Downloaded from www.Manualslib.com manuals search engine

The completed ruleset should look like Figure 7-100.

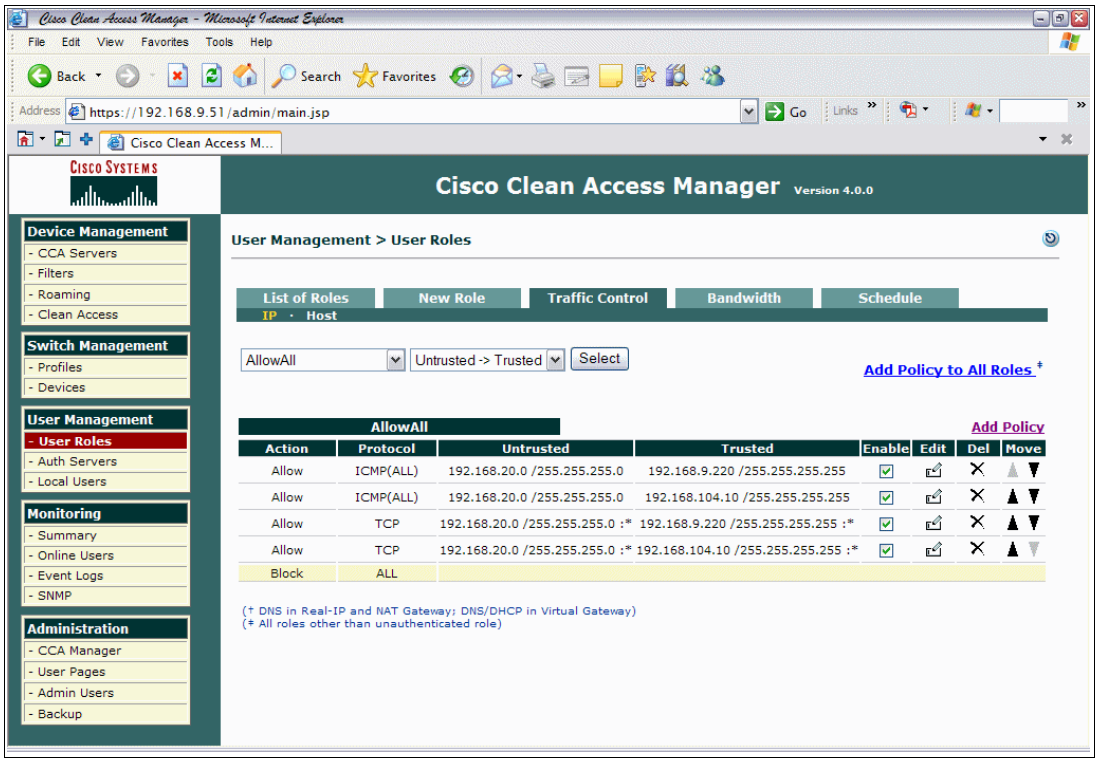


Figure 7-100 Untrusted → Trusted rule creation

11. Repeat steps 6 through 10 for the *quarantine role* and *temporary role*. Users in this scenario, utilizing CCA, are placed in the temporary role if noncompliant. The quarantine role is used for users not passing a network scan, which is out of the scope of this guide.

Note: The rules used here are specific to our lab environment. Think carefully about what rules will need to be used in your own environment, such as DNS, DHCP, different subnets and hosts.

Creating local users

CAM has the ability to perform user authentication using a variety of methods, such as RADIUS, LDAP, Active Directory SSO, and so on.

For the purposes of this book, we use local database authentication.

1. Click **User Management → Local Users → New Local User**.

Downloaded from www.Manualslib.com manuals search engine

2. Add the *user name*, *password*, and *description* as appropriate. From the Role drop-down menu, select which role this user should be mapped to (Figure 7-101).

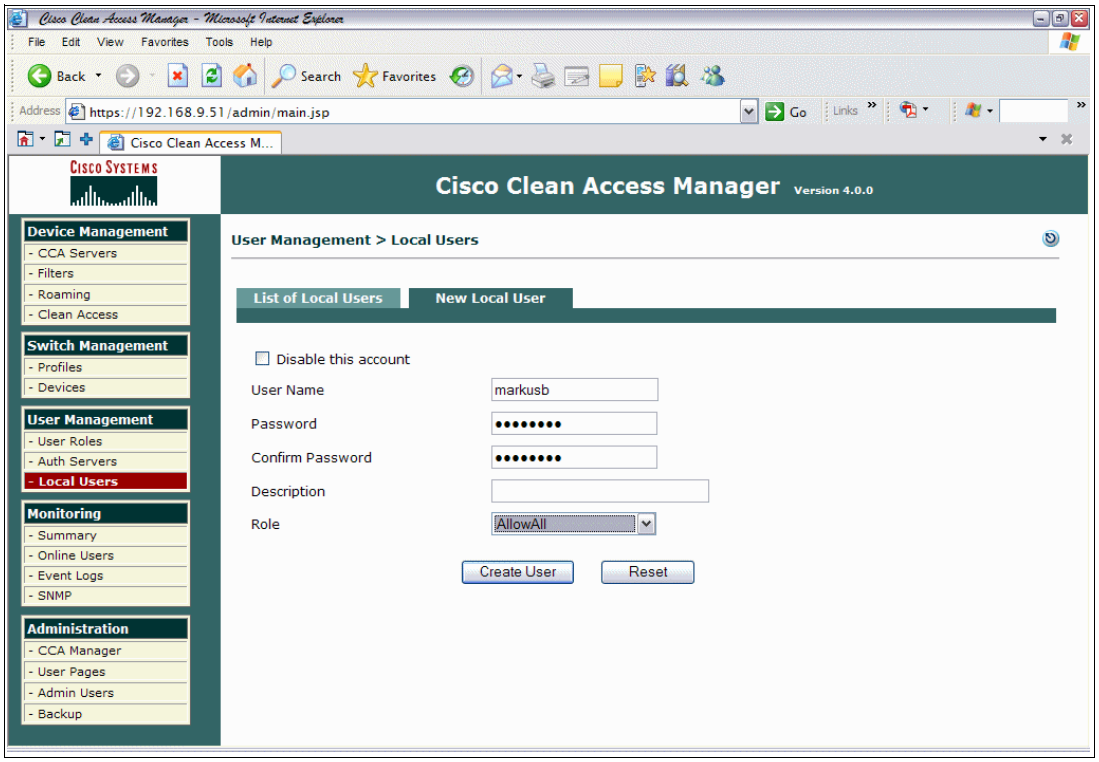


Figure 7-101 Creating a new user

3. Click **Create User**.

Downloaded from www.Manualslib.com manuals search engine

4. The user just created should be seen under *List of Local Users*, as shown in Figure 7-102.

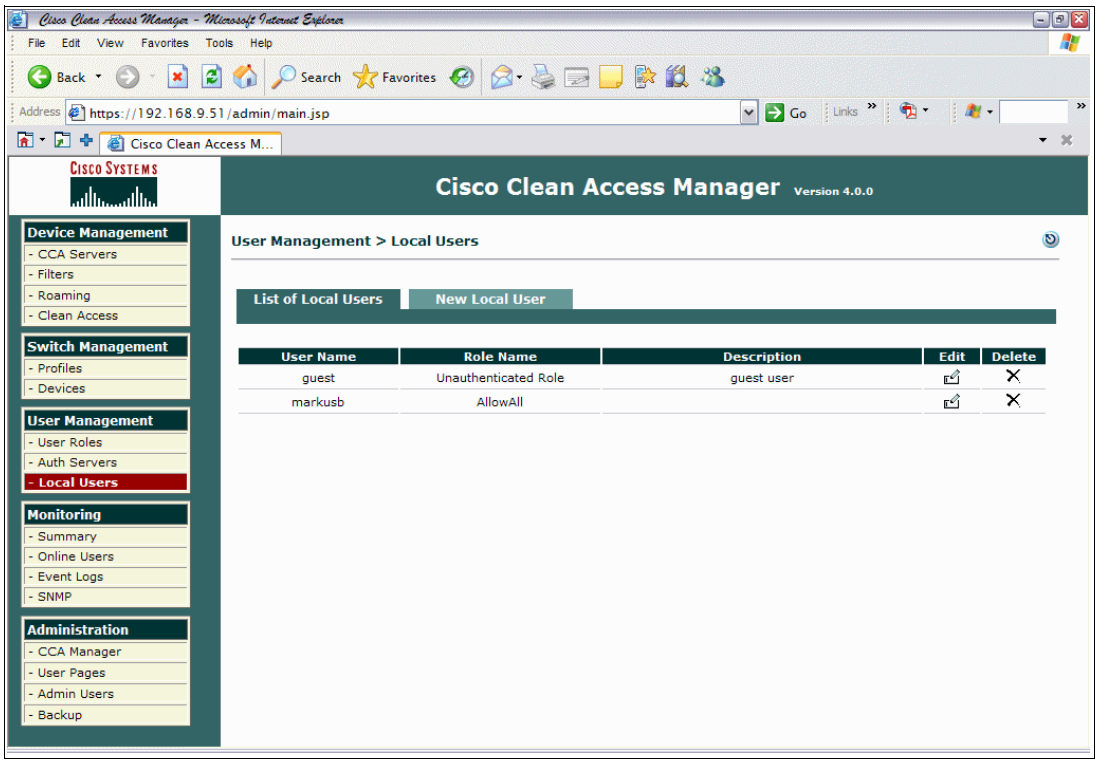


Figure 7-102 List of local users

Configure Clean Access Agent

This section identifies rules and checks that will be applied to users that are running a prototype interface especially designed to interoperate with the Tivoli Security Compliance Manager client for the purpose of this book. NAC Appliance 4.1, scheduled for release before the end of 2006, will contain a feature called *Launch* that can be configured to trigger the Tivoli Security Compliance Manager client. For information about establishing this feature in NAC Appliance please review “NAC Appliance details” on page 455. To configure the Clean Access Agent follow these steps:

1. Click **Device Management** → **Clean Access** → **Clean Access Agent** → **Rules** → **New Check**.

Downloaded from www.Manualslib.com manuals search engine

2. Select the following options (Figure 7-103):
   - From the Check Category drop-down menu, select **Service Check**. The screen will refresh and the Check Type should be set to Service Status.
   - Check Name should be set to SCM_Service.
   - Service Name should be set to jacservice.
   - Operator should be set to running.
   - Check Description should be set to SCM_Service.
   - Operating System should have Windows XP checked.

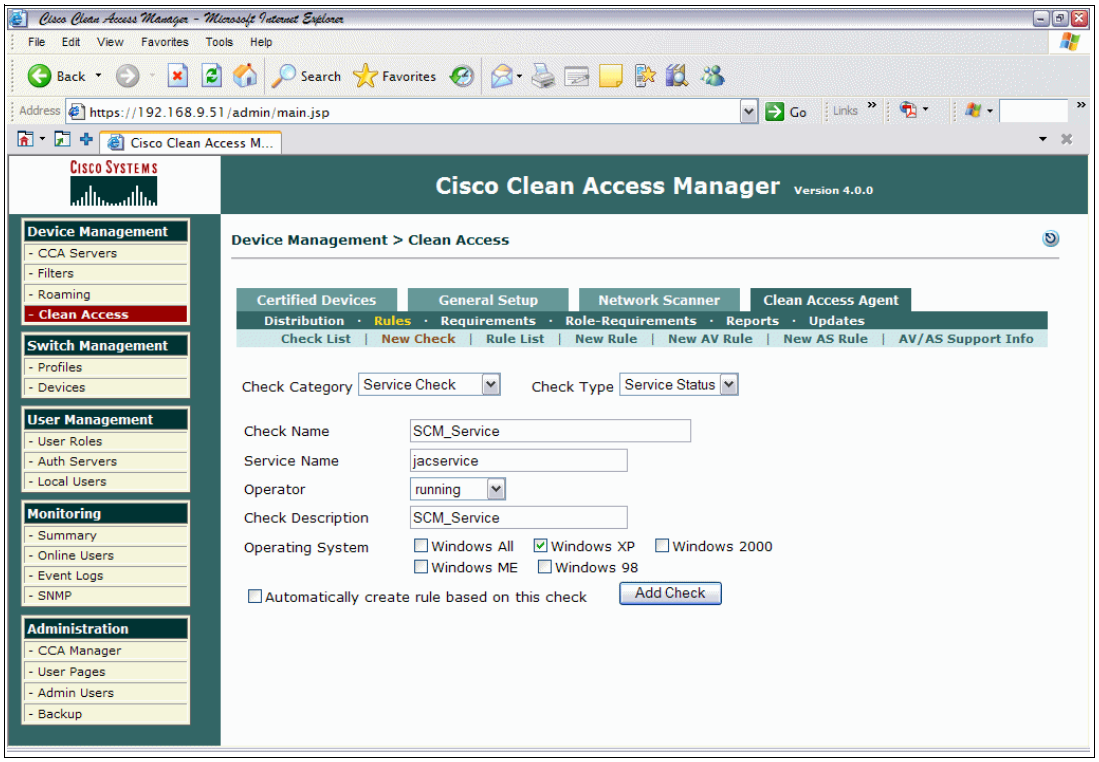


Figure 7-103 Security Compliance Manager Service check

3. Click **Add Check**.
4. Repeat steps 1 and 2, using the following information:
   - From the Check Category drop-down menu, select **Registry Check**. The screen will refresh and the Check Type should be set to Registry Value.
   - Check Name should be set to CCA_Compliance.
   - From the Registry Key drop-down menu, select **HKLM**. The path should be entered as:

     `\SOFTWARE\Cisco\Clean Access Agent`

Downloaded from www.Manualslib.com manuals search engine

- Value Name should be set to Version.
- Value Data Type should be set to String.
- Operator should be set to equals.
- Value Data should be set to 4.0.1.1
- Check Description should be set to CCA_Compliance.
- Operating System should have Windows XP checked (Figure 7-104).

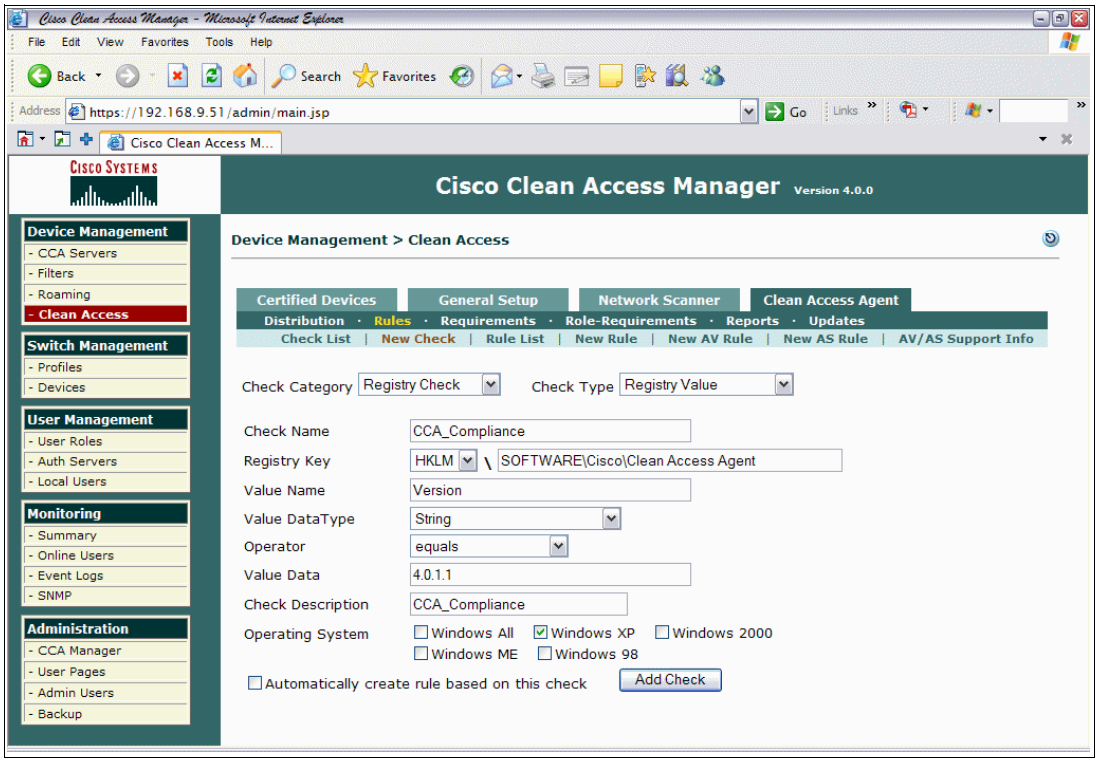


Figure 7-104 CCA version compliance check

5. Click **Add Check**.

Downloaded from www.Manualslib.com manuals search engine

6. These two checks should now be displayed (Figure 7-105).

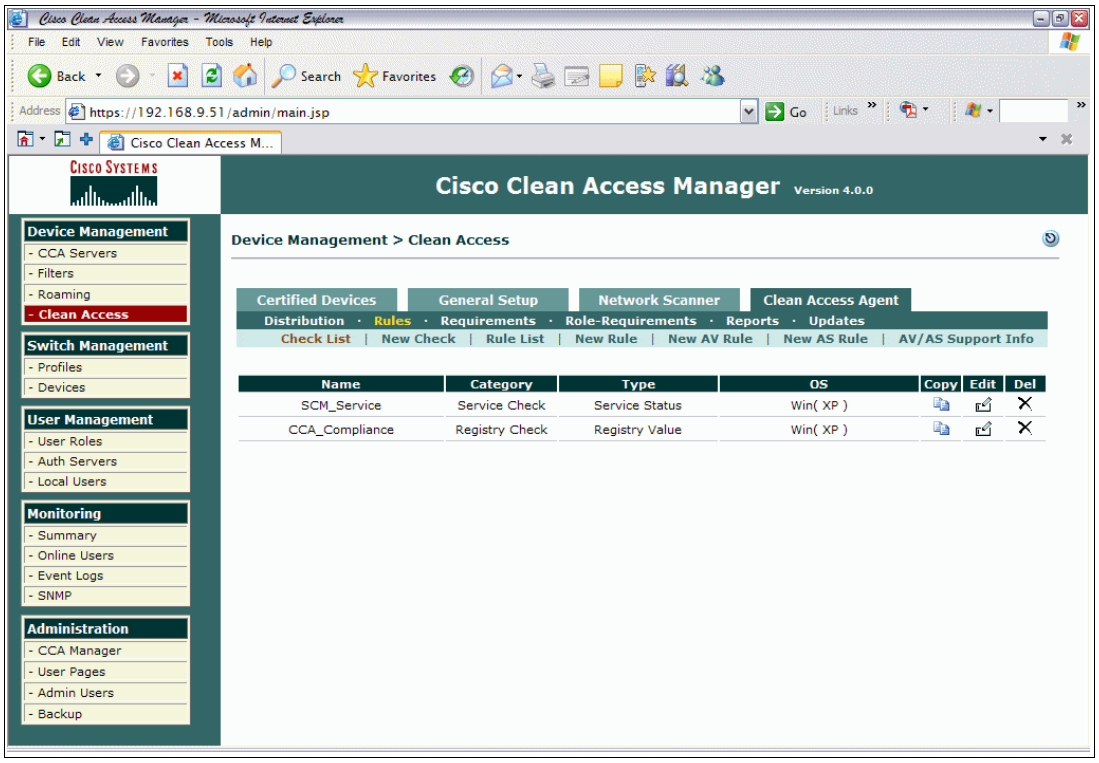


Figure 7-105 Rules check list check

Downloaded from www.Manualslib.com manuals search engine

7. Click **New Rule** (Figure 7-106).

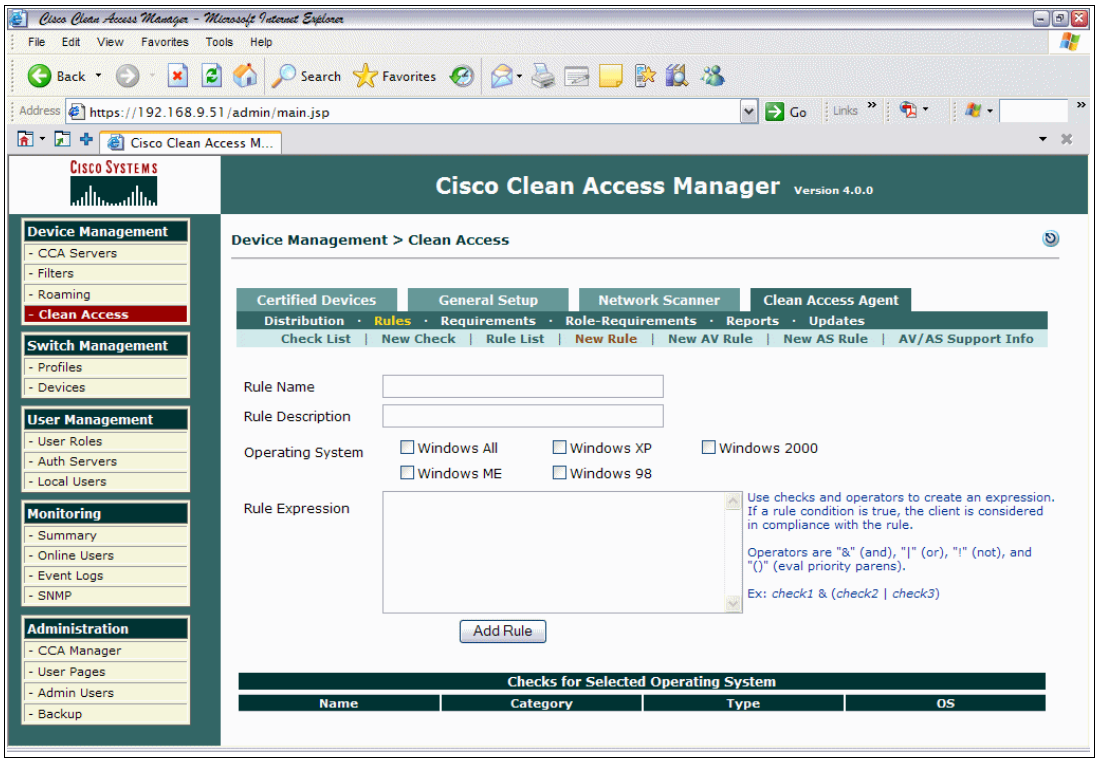


Figure 7-106 New rule

8. Enter the following information:

Rule Name	SCM_Service
Rule Description	Tivoli SCM Service
Operating System	Windows XP checked
Rule Expression®	SCM_Service

9. Click **Save Rule**.

Downloaded from www.Manualslib.com manuals search engine

10. Repeat steps 7 and 8, entering the following information (Figure 7-107):

Rule Name	CCA_Compliance
Rule Description	Cisco Clean Access Agent version
Operating System	Windows XP
Rule Expression	CCA_Compliance

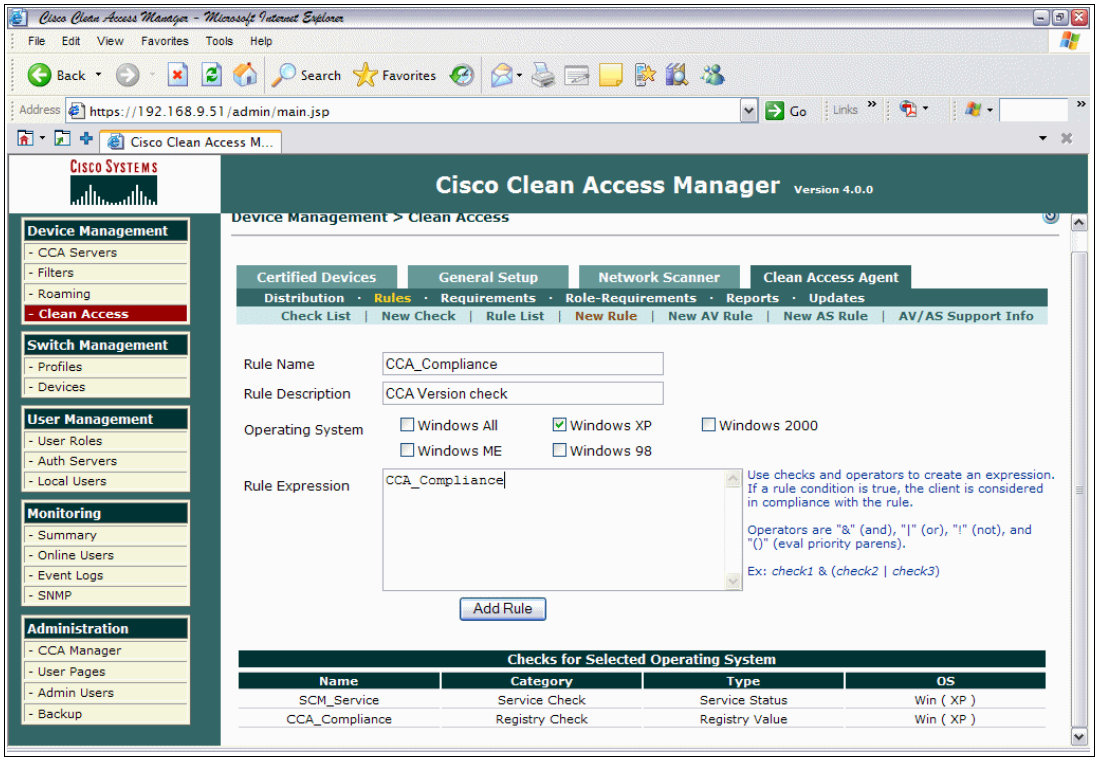


Figure 7-107 CCA Compliance rule definition

11. Click **Add Rule**.

Downloaded from www.Manualslib.com manuals search engine

12. The newly defined rules will be displayed (Figure 7-108).

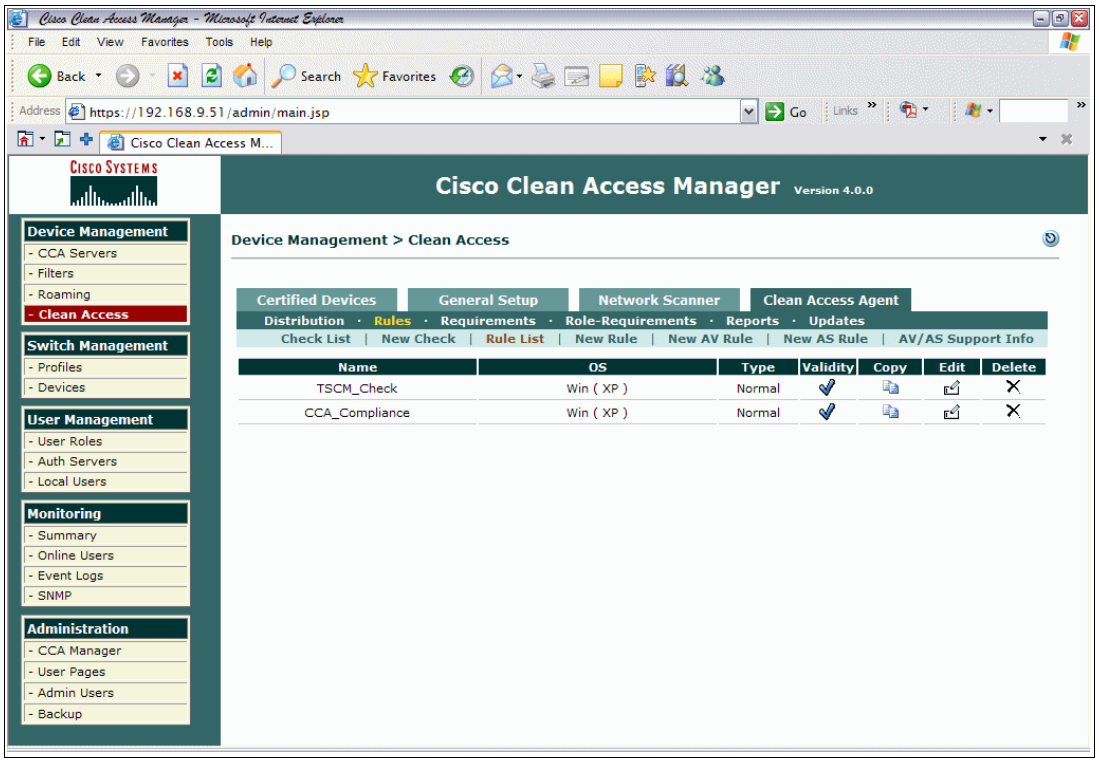


Figure 7-108 New rules

13. Note that both the rules have a blue tick under *Validity*.

Downloaded from www.Manualslib.com manuals search engine

14. Click **Requirements** → **New Requirements** (Figure 7-109).

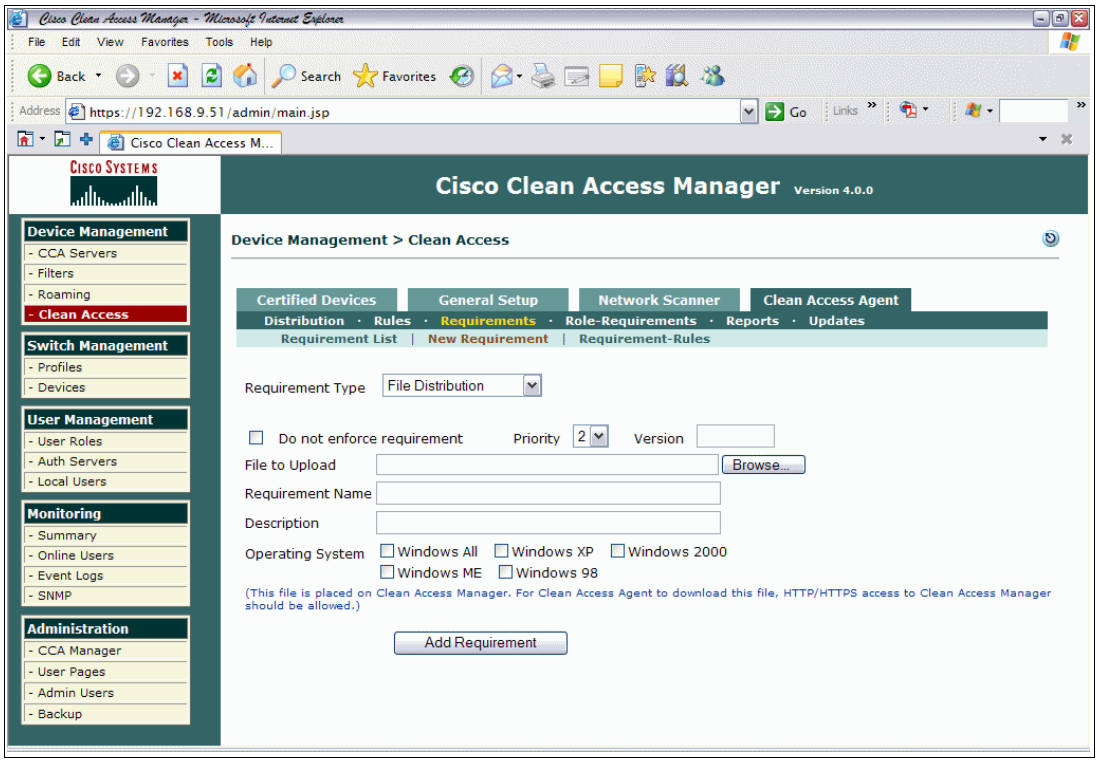


Figure 7-109 Requirements

15. Enter the following information:
    - From the Requirement Type drop-down menu, select **IBM Tivoli SCM**.
    - Set the Priority to 1.
    - For Requirement Name, enter `IBM Tivoli SCM`.
    - For Description, enter `Click [Update] to activate Tivoli SCM remediation and click [Next] after remediation has completed.`
    - Operating System should be set to Windows XP.
16. Click **Add Requirement**.

Downloaded from www.Manualslib.com manuals search engine

17. Repeat steps 14 and 15, entering the following information (Figure 7-110):
    - From the Requirement Type drop-down menu, select **IBM Tivoli SCM**.
    - Set the Priority to 2.
    - For Requirement Name, enter `CCA_Compliance`.
    - For Description, enter `CCA Version compliance`.
    - Operating System should be set to Windows XP.

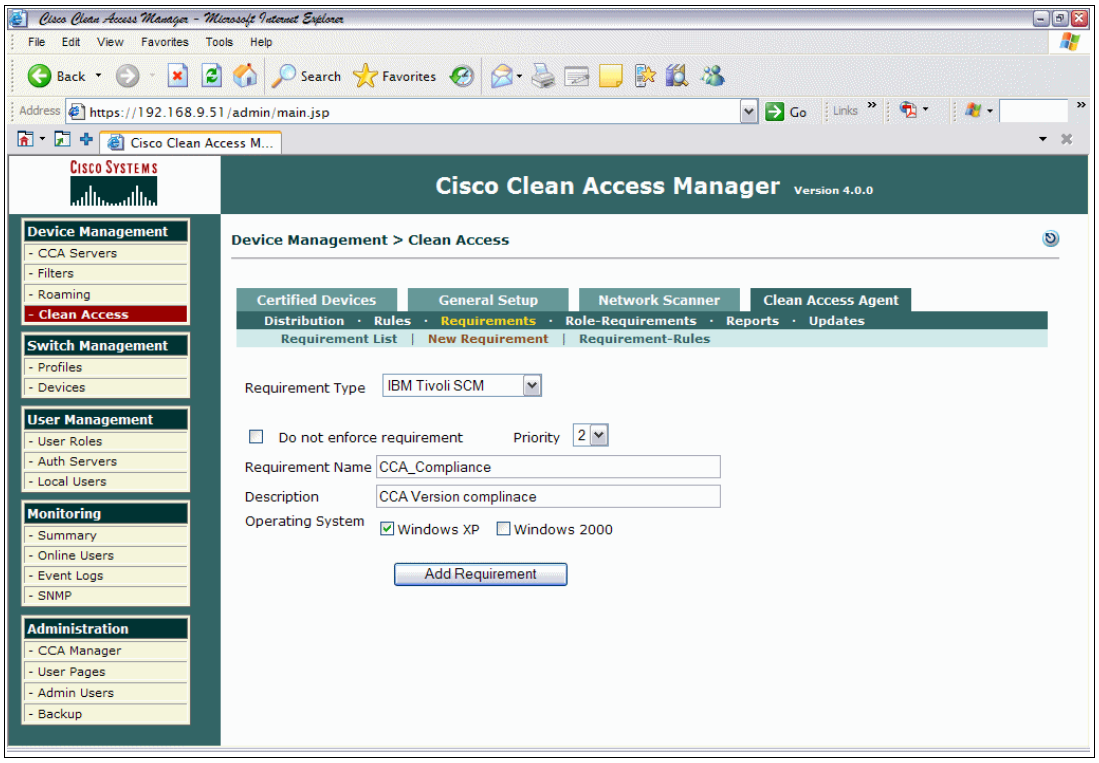


Figure 7-110 CCA Agent update

18. Click **Add Requirement**.

Downloaded from www.Manualslib.com manuals search engine

19. The Requirement List window should appear similar to Figure 7-111.

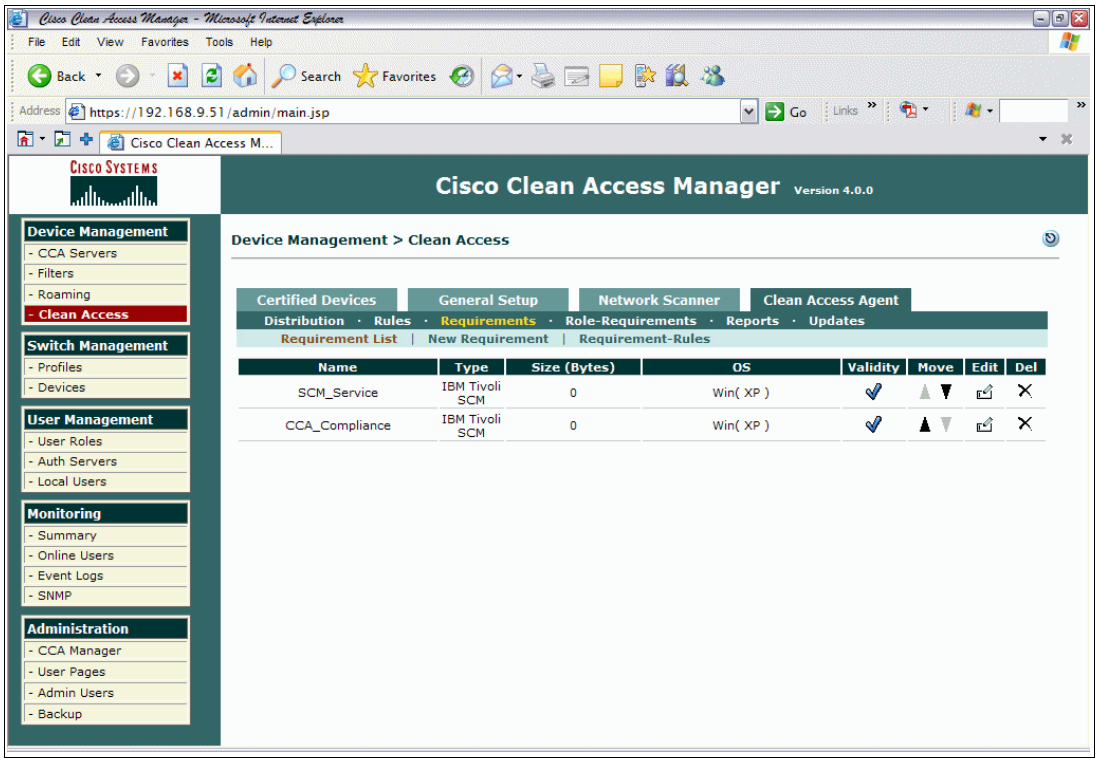


Figure 7-111 Requirements list

20. Click **Requirement Rules**.

21. Enter the following information:

- From Requirement Name, select **SCM_Service**.
- From Operating System, select **Windows XP**.
- From Rules for Selected Operating System, check the box **SCM_Service**.
- Click **Update**.

Downloaded from www.Manualslib.com manuals search engine

22. Repeat steps 20 and 21, entering the following information (Figure 7-112):
    - From Requirement Name, select **CCA_Compliance**.
    - From Operating System, select **Windows XP**.
    - From Rules for Selected Operating System, check the box **CCA_Compliance**.
    - Click **Update**.

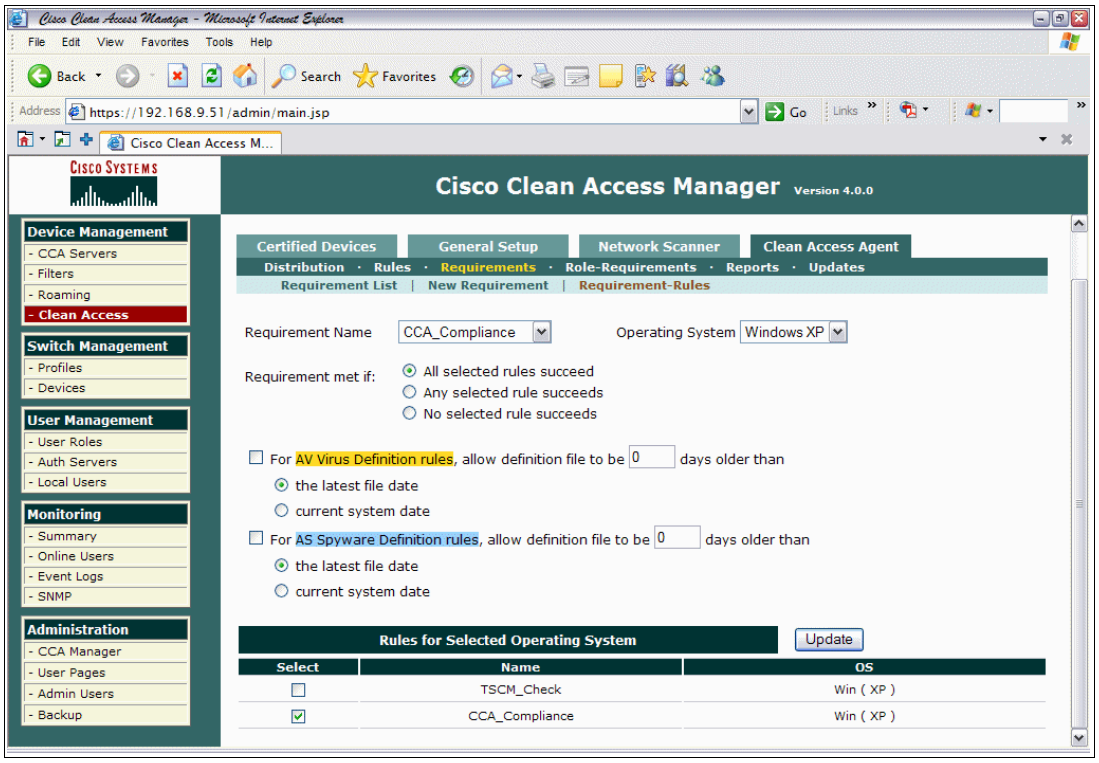


Figure 7-112 CCA Compliance Requirement rule

23. Click **Role-Requirements**.
24. From Role-Type, select **Normal Login Role**, and from User-Role select **AllowAll**.

Downloaded from www.Manualslib.com manuals search engine

25. From “Select requirements to associate with the role,” select both **SCM_Service** and **CCA_Compliance** (Figure 7-113).

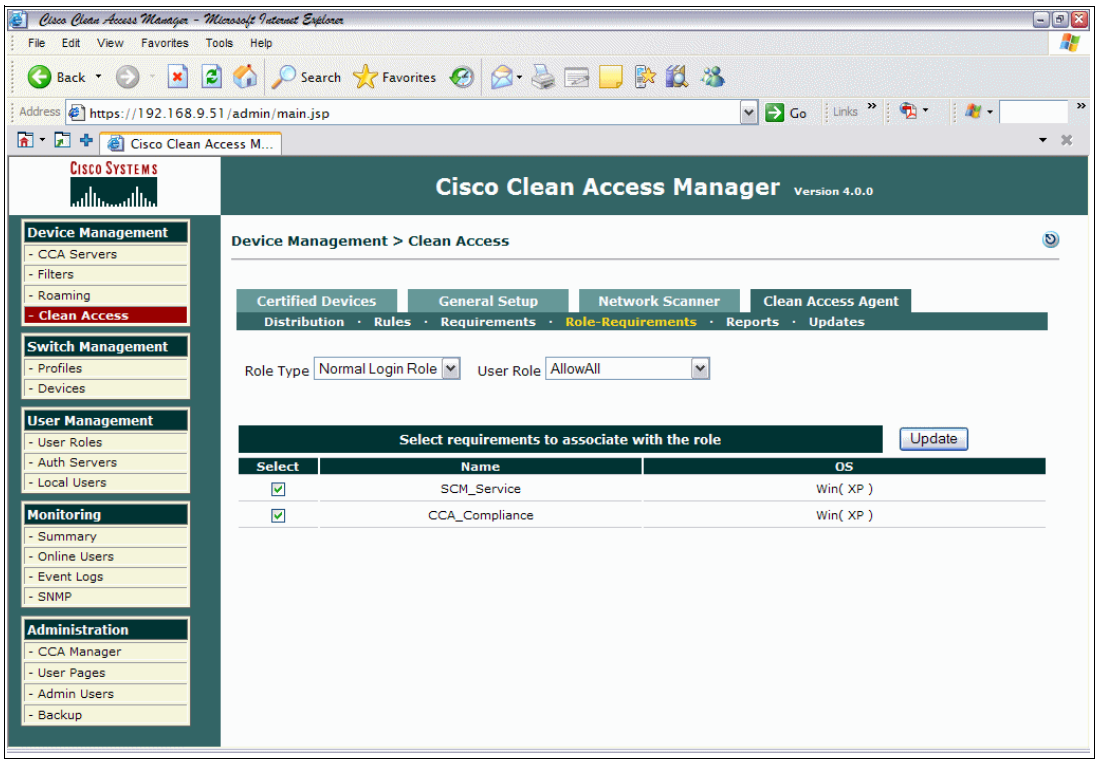


Figure 7-113 Role requirements

26. Click **Update**.

Downloaded from www.Manualslib.com manuals search engine

Discovered clients

To check that the Clean Access Solution is working properly, select **View Online Users** → **Out-of-Band** (Figure 7-114).

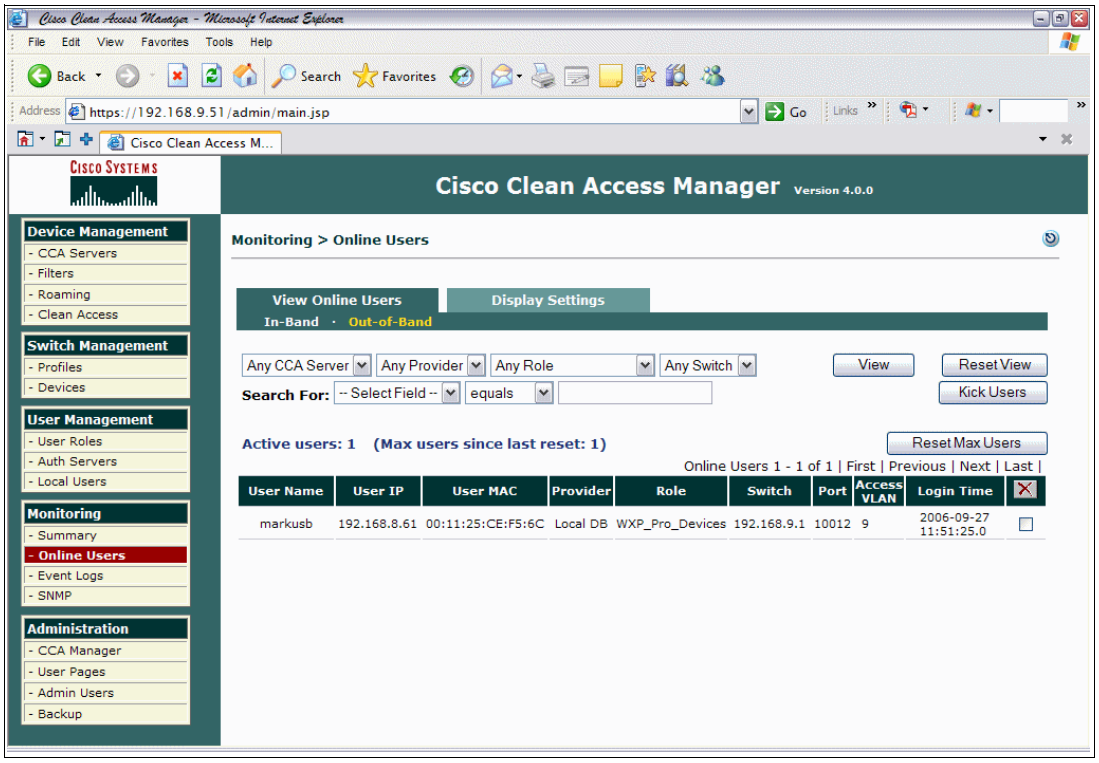


Figure 7-114 Viewing online users

Downloaded from www.Manualslib.com manuals search engine

Logging on as a client

To log on as a client follow these steps.

1. Once the CCA Agent software has been installed on the client machine, the user will be prompted for their user name and password (Figure 7-115).

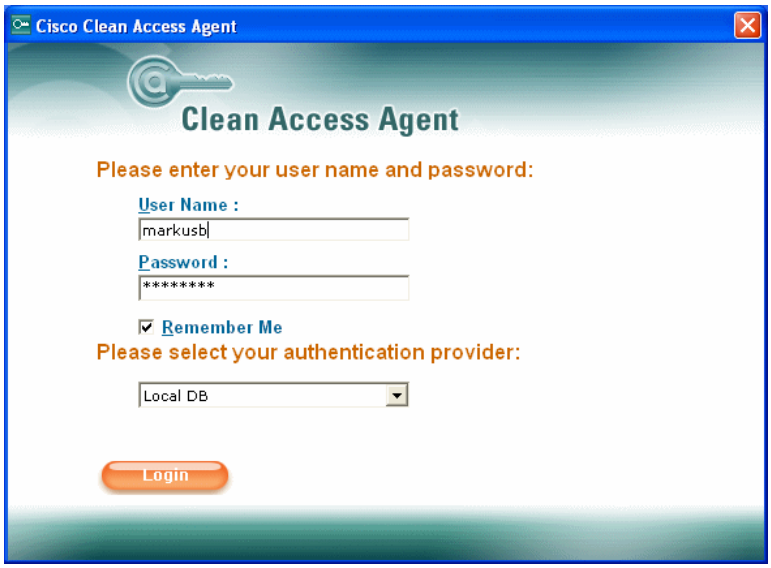


Figure 7-115 Client log-in screen

2. Click **Login**.
3. If the client is healthy, it will be granted access to the network (Figure 7-116).

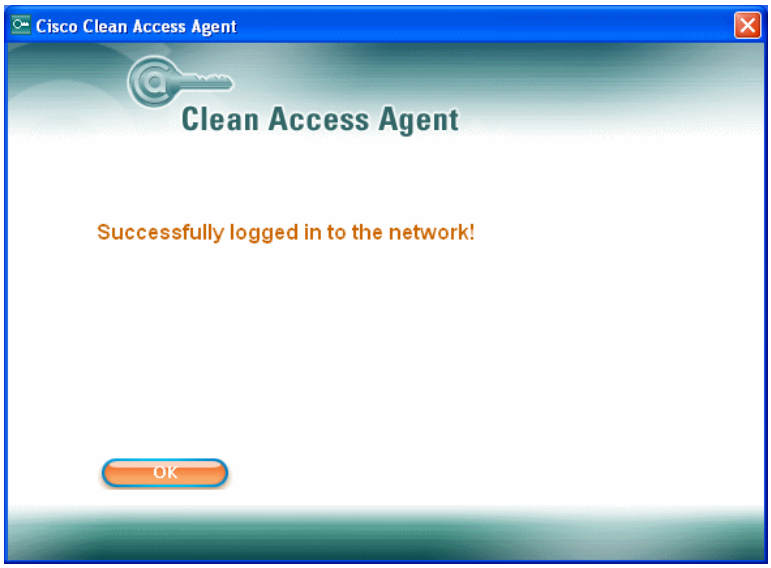


Figure 7-116 Successful login

Downloaded from www.Manualslib.com manuals search engine

4. Click **OK**.
5. If a client fails the compliance check, a Web page will pop-up notifying the user that he is noncompliant (Figure 7-117).

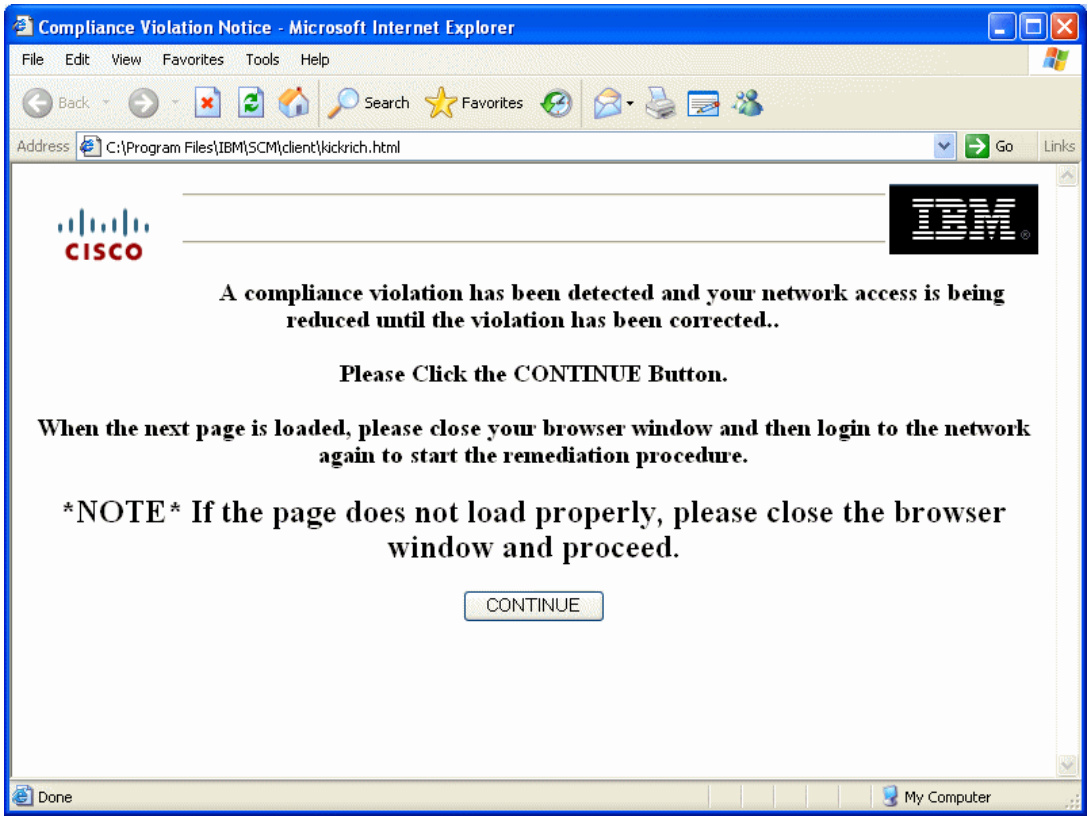

Compliance Violation Notice - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Program Files\IBM\SCM\client\kickrich.html
Go Links
CISCO
IBM
A compliance violation has been detected and your network access is being reduced until the violation has been corrected..
Please Click the CONTINUE Button.
When the next page is loaded, please close your browser window and then login to the network again to start the remediation procedure.
NOTE If the page does not load properly, please close the browser window and proceed.
CONTINUE
Done
My Computer

Figure 7-117 Web page pop-up informing user about non-compliance

6. Click **Continue**.
7. The user is disconnected from the network, and then reconnected, forcing him to log back in to CCA. The user enters the credentials as per Figure 7-115 on page 347, and clicks **Login**.

Downloaded from www.Manualslib.com manuals search engine

8. The user is advised of their temporary access (Figure 7-118), and clicks **Continue**.

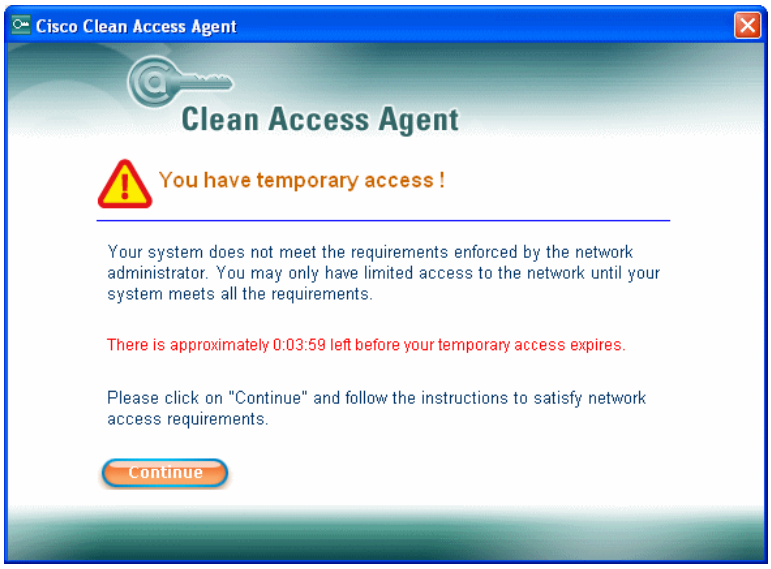

Cisco Clean Access Agent
Clean Access Agent
You have temporary access !
Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.
There is approximately 0:03:59 left before your temporary access expires.
Please click on "Continue" and follow the instructions to satisfy network access requirements.
Continue

Figure 7-118 Temporary access notification

9. User clicks **Update** (Figure 7-119).

Figure 7-119 Required software notification screen

Downloaded from www.Manualslib.com manuals search engine

10. The Security Compliance Manager Compliance Report window pops up (Figure 7-120). In this example we can see that there is a policy violation with the user password settings.

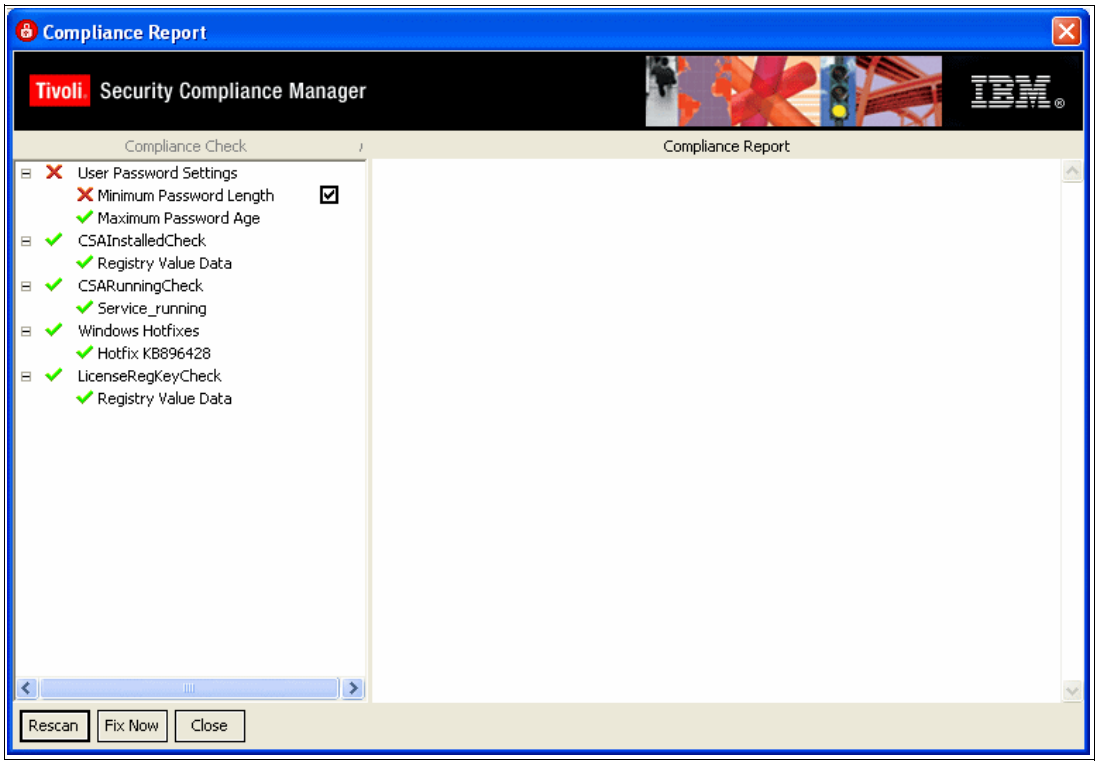


Figure 7-120 Security Compliance Manager Compliance Report window

11. User clicks **Fix Now**.

12. A remediation pop-up window informs the user that the remediation has finished, and the user clicks **OK** (Figure 7-121).

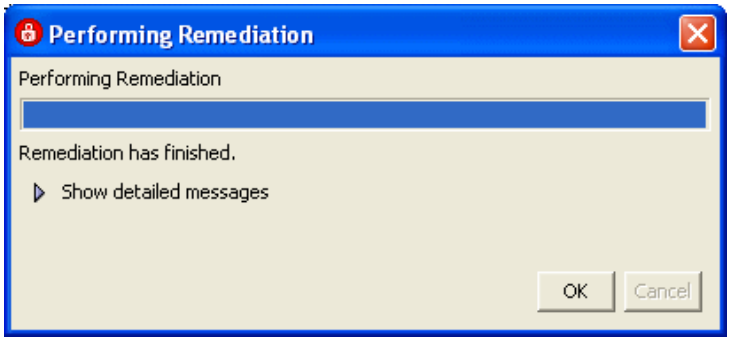


Figure 7-121 Remediation notification

Downloaded from www.Manualslib.com manuals search engine

13. The user clicks **Close** on the Security Compliance Manager Compliance Report window, which shows all items in a state of *green tick* compliance (Figure 7-122).

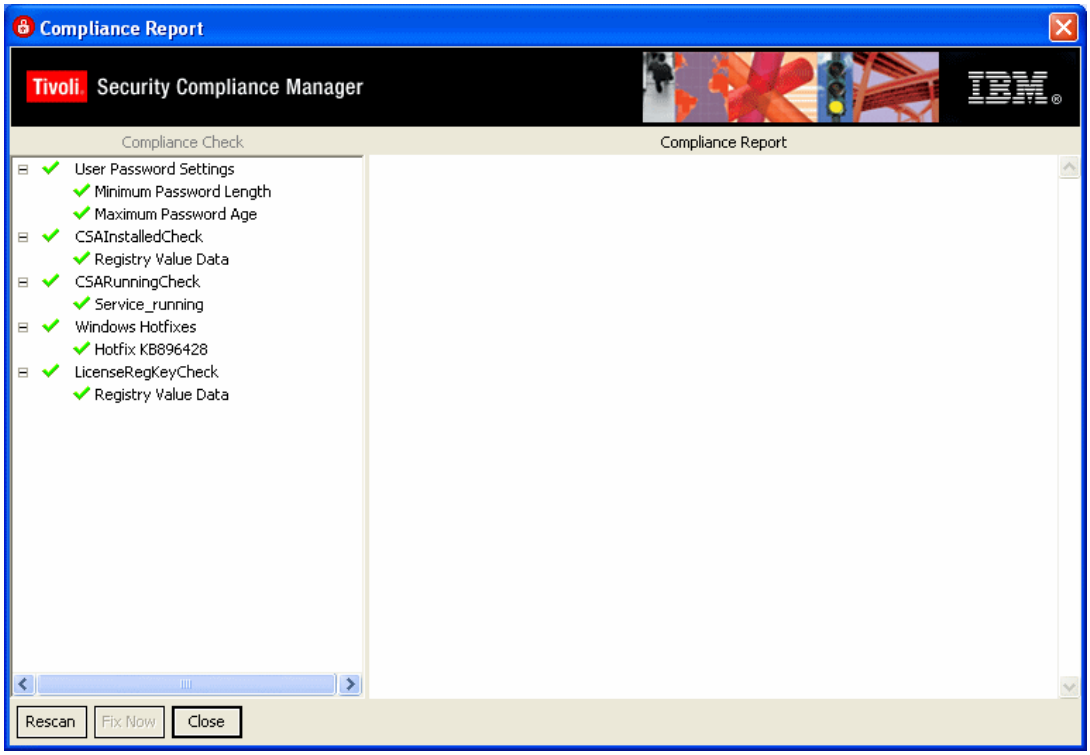


Figure 7-122 Security Compliance Manager Compliance Report window - all compliant

14. The user clicks **Next** from the screen shown in Figure 7-119 on page 349.

Downloaded from www.Manualslib.com manuals search engine

15. The end user is advised of successful login to the network (Figure 7-123).

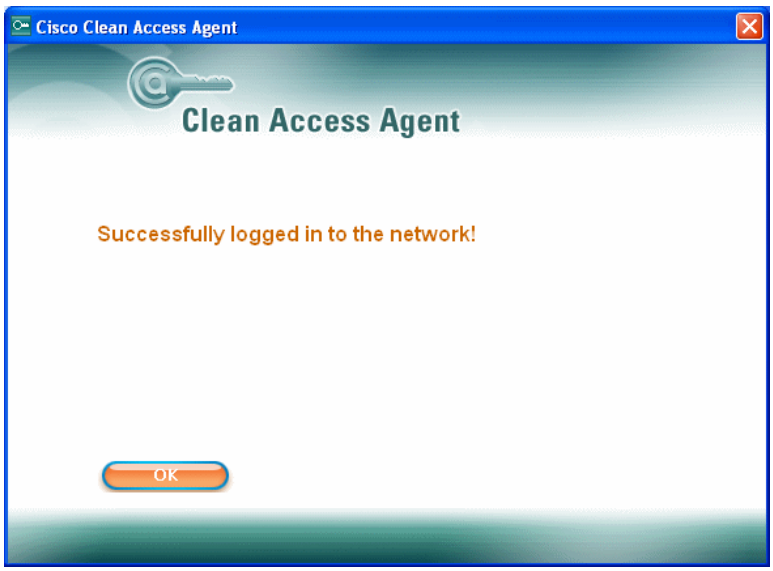


Figure 7-123 Successful login

This concludes the basic configuration requirements for the CAREx on the CAM.

7.2.3 Deployment of the network infrastructure

In this section we describe how to configure the Cisco Catalyst 3750 switch for implementation in a NAC Appliance environment.

Configuring Cisco 3750 switch for NAC Appliance

NAC Appliance OOB only works with Cisco switches. If you are using hardware other than Cisco, this solution can still be deployed, but as in-band, which is beyond the scope of this book. For more information about switch compatibility for NAC Appliance refer to:

http://www.cisco.com/en/US/partner/products/ps6128/products_device_support_table09186a00806f65fb.html

Example interface configuration for a NAC Appliance client:

```
interface FastEthernet1/0/12
 description **Test CCA Client port**
 switchport access vlan 20
 switchport mode access
 snmp trap mac-notification added
 spanning-tree portfast
!
```


Downloaded from www.Manualslib.com manuals search engine

Example of interface configuration for CAM interface:

```
interface FastEthernet1/0/18
 description **CAM Interface**
 switchport access vlan 9
 switchport mode access
 spanning-tree portfast
!
```

Example of interface configuration for Untrusted CAS interface:

```
interface FastEthernet1/0/4
 description **Untrusted Interface CCA Server**
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 998
 switchport trunk allowed vlan 120,998
 switchport mode trunk
 spanning-tree portfast
!
```

Example of interface configuration for Trusted CAS interface:

```
interface FastEthernet1/0/16
 description **Trusted Interface CCA Server**
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,999
 switchport mode trunk
 spanning-tree portfast
!
```

Example of VLAN/SVI configuration:

```
interface Vlan9
 ip address 192.168.9.1 255.255.255.0
!
interface Vlan10
 ip address 192.168.10.7 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan120
 no ip address
!
interface Vlan998
 no ip address
!
interface Vlan999
 no ip address
!
```


Downloaded from www.Manualslib.com manuals search engine

Example of SNMP configuration:

```
snmp-server community public RW
snmp-server community c3750_read RO
snmp-server location Matanzas
snmp-server contact Admin
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server host 192.168.9.51 public  mac-notification snmp
```

7.3 Conclusion

In this chapter we presented the essential steps to build and configure a Network Admission Control solution for both NAC Framework and NAC Appliance approaches. We covered the installation and configuration for required client and server components and the router and switch configuration.

At this point we have finished the setup of the basic compliance and network enforcement subsystem. The configuration of the remediation subsystem is covered in Chapter 8, “Remediation subsystem implementation” on page 355.

Downloaded from www.Manualslib.com manuals search engine

8

Remediation subsystem implementation

This chapter describes the IBM Tivoli Configuration Manager part of the Network Admission Control (NAC) solution, where the main concern is the remediation of the noncompliant clients. The remediation process can be either manual, done by the user who follows provided instructions, or automated, where the user only clicks the Fix Now button in the provided user interface.

We also discuss the maintenance issues with the solution components and provide a detailed walkthrough for remediation workflow creation to match the security policy change process.

Creating the automated remediation component requires the following components and tasks:

- Installation and configuration of the Tivoli Configuration Manager Web Gateway on top of the base Tivoli Configuration Manager server.
- Creating the remediation instructions for the users based on input data from the security-compliance team about the configuration of the compliance policy.
- Remediation server configuration. This includes several steps:
  - Installation of the Software Package Web Server
  - Configuration of the Software Package Web Server

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

- Installation of the software package utilities
- Creating remediation workflows that matches Security Compliance Manager policies with the suitable remediation workflow names and parameters

Downloaded from www.Manualslib.com manuals search engine

8.1 Automated remediation enablement

To enable automated remediation, the remediation handler that is automatically installed on the client with the *policy collector* has to be properly configured. As opposed to the first release of the remediation solution where an SSH protocol was used, this release of the IBM Integrated Security Solution for Cisco Networks relies on the HTTP protocol to download remediation packages from the remediation server. It also uses a pull method instead of a push method used with the previous release when the Tivoli Provisioning Manager was used for remediation. This change greatly enhances the scalability of the solution.

The remediation solution on the client consists of three parts:

- Default remediation handler
- Tivoli Configuration Manager remediation handler
- Tivoli Configuration Manager standalone commands

The default remediation handler is a part of the *com.ibm.scm.nac.posture.PolicyCollector* and is responsible for presenting to the end user the status of the posture check. When armed with the additional HTML pages as described in 8.3, “Creating remediation instructions for the users” on page 397, it can also provide an explanation of the current security policy as well as remediation instructions to the user.

The Tivoli Configuration Manager remediation handler is an additional Java class that is called when the user clicks the Fix Me button in the interface presented by the default remediation handler. This element is responsible for connecting to the Software Package Web Server and downloading the correct remediation package. It is delivered to the client in the form of the Tivoli Security Compliance Manager collector named *com.ibm.scm.nac.tcmremed.client.TCMRemed*.

Next the Tivoli Configuration Manager commands are called to install the package on the local machine. Since the software package block (SPB) is a very flexible format it may include running any command on the system, changing the configuration files or Windows registry. The set of Tivoli Configuration Manager commands designed to handle SPB files is delivered to the client with the special TCMCLI policy described in “TCMCLI utility policy” on page 189.

Summarizing the above, the following conditions have to be met in order for an automated remediation to be available:

1. The Tivoli Security Compliance Manager client has to be assigned with two policies. One of them must include *com.ibm.scm.nac.posture.PolicyCollector* and *com.ibm.scm.nac.tcmremed.client.TCMRemed* collectors. The second must be the TCMCLI policy available for import in the *IISSCN extension pack2*

Downloaded from www.Manualslib.com manuals search engine

for Tivoli Configuration Manager package at the IBM Tivoli Security Compliance Manager 5.1 Utilities page at the following link:

http://www.ibm.com/support/docview.wss?uid=swg24007082

2. The *com.ibm.scm.nac.posture.PolicyCollector* has to be configured with the following parameters:
   - REMEDIATION_JAR equal to collectors/com.ibm.scm.nac.tcmremed.client.TCMRemed.jar
   - REMEDIATION_CLASS equal to com.ibm.scm.nac.tcmremed.client.TCMRemediator
   - HANDLER_ATTRIBUTES equal to remediation.url=http://<name_of_the_remediation_server>/SoftwarePackageServerWeb/SPServlet

In the current release all of the required files for automatic remediation are collectors and are part of the policy, so they are downloaded and maintained automatically from the Security Compliance Manager server when the policy is assigned to the client. The steps required to properly set up the client workstation are described in 6.3, “Deploying the client software” on page 189.

8.2 Remediation server software setup

To get started with the automated remediation process, we must understand the proper prerequisites before setting up the Tivoli Configuration Manager.

8.2.1 Prerequisites

To properly set up all server components required for the automated remediation, you must install additional installation media:

- For Tivoli Configuration Manager server 4.2.3 base installation:
  - Tivoli Configuration Manager Installer 4.2.3
  - DB2 Version 8.2
  - Tivoli Configuration Manager server 4.2.3
  - Tivoli Framework 4.1.1 CD1
  - Tivoli Framework 4.1.1 CD2
- For Tivoli Configuration Manager Web Gateway installation:
  - WebSphere Application Server 5.1 or later
  - Tivoli Configuration Manager Web Gateway 4.2.3

Downloaded from www.Manualslib.com manuals search engine

- For Software Package Web Server component:

  The *IISSCN enablement pack2 for Tivoli Configuration Manager* package available on the IBM Tivoli Security Compliance Manager 5.1 Utilities Web site:

  `http://www.ibm.com/support/docview.wss?uid=swg24007082`

  These are free to download. However, you must have a registered PartnerWorld® or developerWorks® ID to access this site.

We also recommend that you have the *IBM Tivoli Configuration Manager Version 4.2.3: Planning and Installation Guide,* GC23-4702-03, handy.

Important: We emphasize one general note about obtaining the latest fix packs and upgrades: Always check the latest Deployment Guide for the IBM Integrated Security Solution for Cisco Networks to verify the correct software status.

8.2.2 Tivoli Configuration Manager

We assume that you have an installation of the base Tivoli Configuration Manager Version 4.2.3 up and running. In the following sections we cover the installation and configuration of the Web Gateway feature and the setup of a remediation server using these components.

In the next section we describe the detailed walkthrough to prepare the Tivoli Configuration Manager machine for automated remediation.

Tivoli Configuration Manager Web Gateway setup

In our lab we were using Windows 2003 Enterprise Server Service Pack 1as an operating system for Tivoli Configuration Manager server. If UNIX or Linux is your platform of choice, the installation of the Tivoli Configuration Manager Web Gateway will be very similar, except different path settings. The generic description of the installation process can be found in Chapter 6 “Web Gateway Installation” in *IBM Tivoli Configuration Manager Version 4.2.3: Planning and Installation Guide,* GC23-4702-03.

For all of the steps below we assume that you are logged onto the Configuration Manager server with administrative privileges.

Downloaded from www.Manualslib.com manuals search engine

Preparing for the installation

Tivoli Configuration Manager Web Gateway requires several prerequisites to be successfully installed. The following steps must be accomplished before attempting Tivoli Configuration Manager Web Gateway installation:

- Installation of the database server software. In our lab we used DB2 Version 8.2, as this is provided with the Tivoli Configuration Manager software.
- Installation of the Web infrastructure, which is WebSphere Application Server and IBM HTTP server. In our lab we used the versions provided with the Tivoli Configuration Manager software and updated them with the latest fix packs.
- Creation of a user account for database access.

Installation of the DB2 database

The installation of the DB2 database was covered in 6.1.1, “Installation of DB2 database server” on page 126. You may also use the same database that is used by the other components of Tivoli Configuration Manager.

Installation of Web infrastructure

Installation of WebSphere Application Server is a simple process. Below we describe the installation of WebSphere Application Server Version 5.1, which is included with Tivoli Configuration Manager. This process also installs IBM HTTP Server, which plays a role at the front end for incoming HTTP requests.

To perform the installation you need the following media:

- WebSphere Application Server V5.1 for Windows. The product CD is included with your Tivoli Configuration Manager installation bundle.
- WebSphere Application Server V5.1 Fix Pack 1, which can be downloaded from the following IBM Web site:

  `http://www.ibm.com/support/docview.wss?rs=180&uid=swg27004980#ver51`

  Or optionally from the FTP server:

  `ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixpacks/was51/fixpack1`
- WebSphere Application Server V5.1.1 cumulative Fix 11, which can be downloaded from the following IBM Web site:

  `http://www.ibm.com/support/docview.wss?rs=180&uid=swg27004980#ver51`

  Or optionally from the FTP server:

  `ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixpacks/was51/cumulative/cf51111`

Downloaded from www.Manualslib.com manuals search engine

The steps to install the minimal required version of Web infrastructure are:

1. To start the installation go the directory where you have your installation media for WebSphere Application Server 5.1 to the \win subdirectory and run the file LaunchPad.bat.
2. The installation Launchpad window is displayed, as shown on Figure 8-1. Using the launchpad you may easily reach and read the product overview or installation guide. To start the installation wizard click **Install the product**.

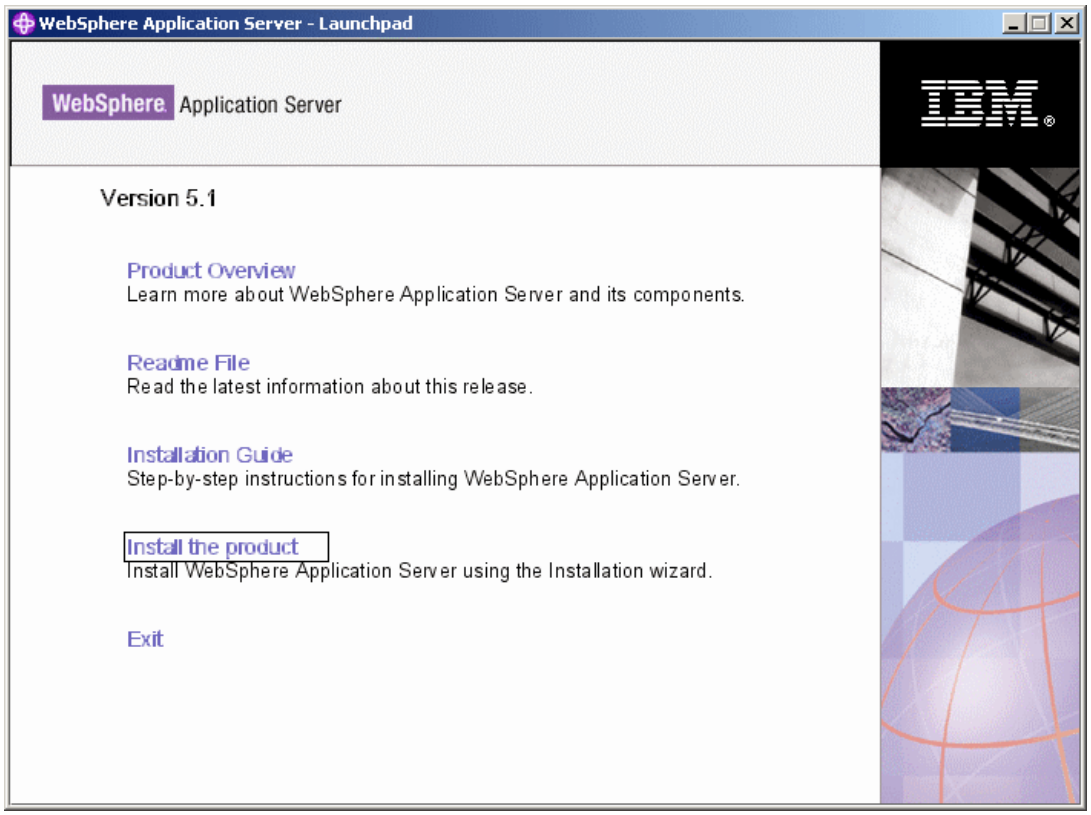

WebSphere Application Server - Launchpad
WebSphere Application Server
IBM
Version 5.1
Product Overview
Learn more about WebSphere Application Server and its components.
Readme File
Read the latest information about this release.
Installation Guide
Step-by-step instructions for installing WebSphere Application Server.
Install the product
Install WebSphere Application Server using the Installation wizard.
Exit

Figure 8-1 WebSphere Application Server launchpad

Downloaded from www.Manualslib.com manuals search engine

3. The WebSphere Application Server Installation wizard is displayed, as shown in Figure 8-2. Click **Next**.

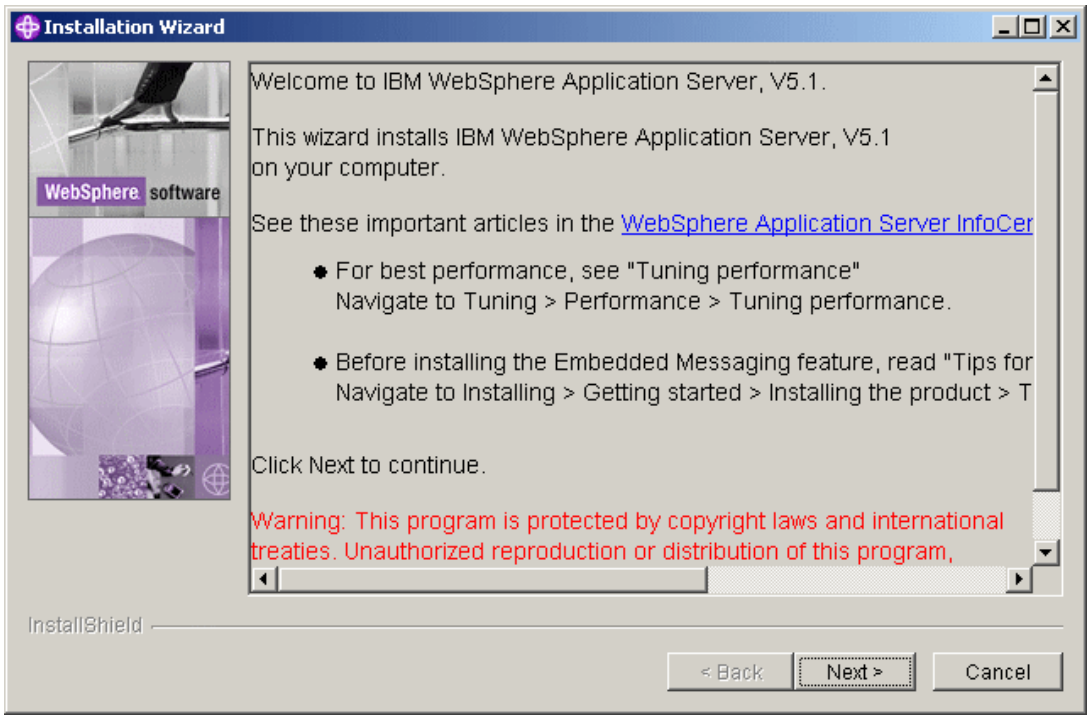

Installation Wizard
WebSphere software
Welcome to IBM WebSphere Application Server, V5.1.
This wizard installs IBM WebSphere Application Server, V5.1
on your computer.
See these important articles in the WebSphere Application Server InfoCer
For best performance, see "Tuning performance"
Navigate to Tuning > Performance > Tuning performance.
Before installing the Embedded Messaging feature, read "Tips for
Navigate to Installing > Getting started > Installing the product > T
Click Next to continue.
Warning: This program is protected by copyright laws and international
treaties. Unauthorized reproduction or distribution of this program,
InstallShield
< Back
Next >
Cancel

Figure 8-2 WebSphere Installation Wizard window

Downloaded from www.Manualslib.com manuals search engine

4. In the next window, the standard license agreement is presented, as shown in Figure 8-3. Accept the license and click **Next**.

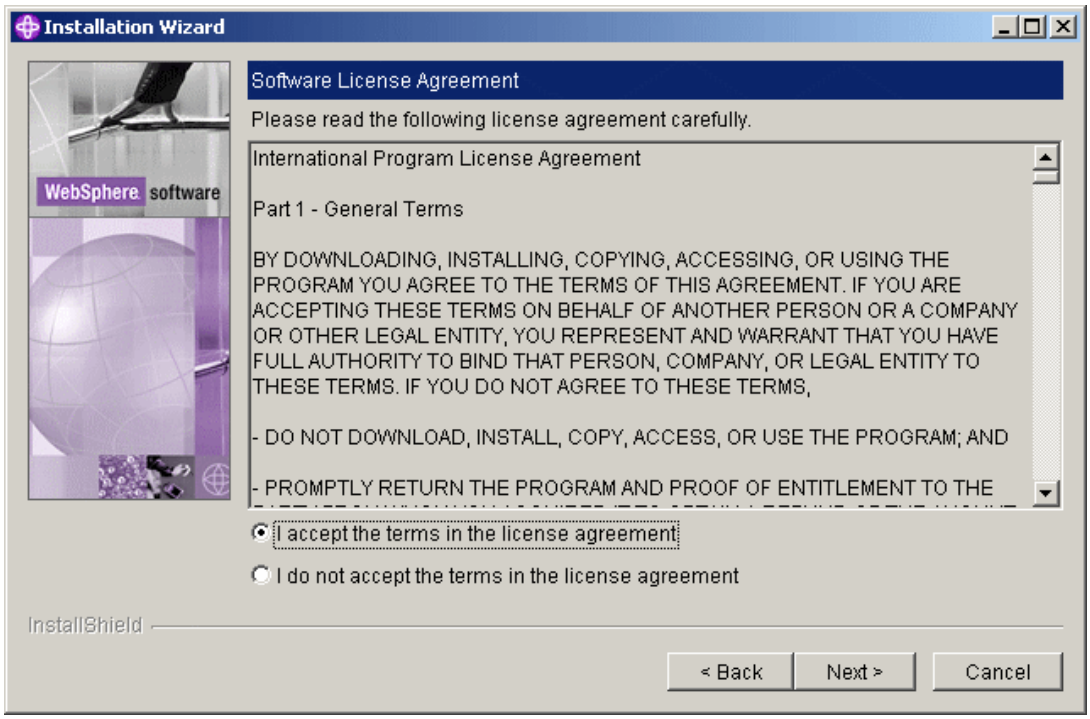

Installation Wizard
WebSphere software
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Figure 8-3 Software License Agreement window

Downloaded from www.Manualslib.com manuals search engine

5. In the next window shown in Figure 8-4 you must select the installation type. For the lab environment we decided to select custom installation to prevent the installation of unnecessary components in order to limit memory usage. If you do not care for memory usage you can follow the full installation path. However, some of the next windows presented in the book may slightly differ. If you want to follow the book select **Custom** and click **Next**.

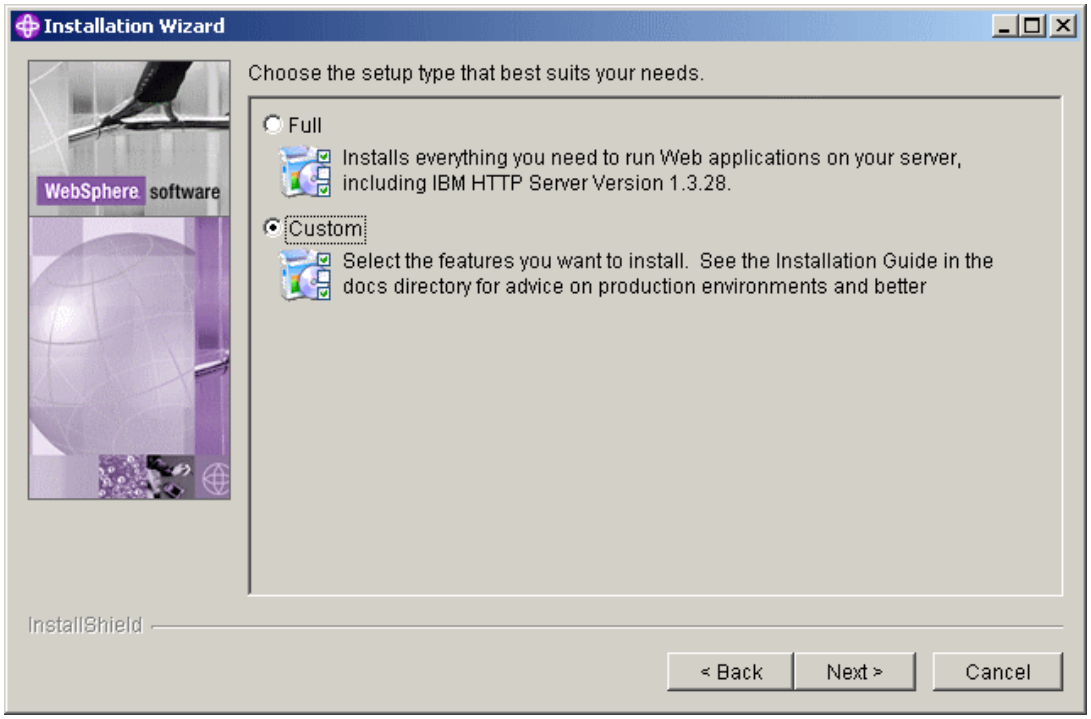

Installation Wizard
WebSphere software
Choose the setup type that best suits your needs.
Full
Installs everything you need to run Web applications on your server, including IBM HTTP Server Version 1.3.28.
Custom
Select the features you want to install. See the Installation Guide in the docs directory for advice on production environments and better
InstallShield
< Back
Next >
Cancel

Figure 8-4 Installation type selection

6. If you have selected the custom install, you must select the components that you want to install in the next window. Deselect everything except:
   - Application Server
   - Administration
     - Scripted Administration
     - Administration Console
   - IBM HTTP Server Version 1.3.28
   - Web server plug-ins
     - Plug-in for IBM HTTP Server v1.3

Downloaded from www.Manualslib.com manuals search engine

This is shown in Figure 8-5. Click **Next**.

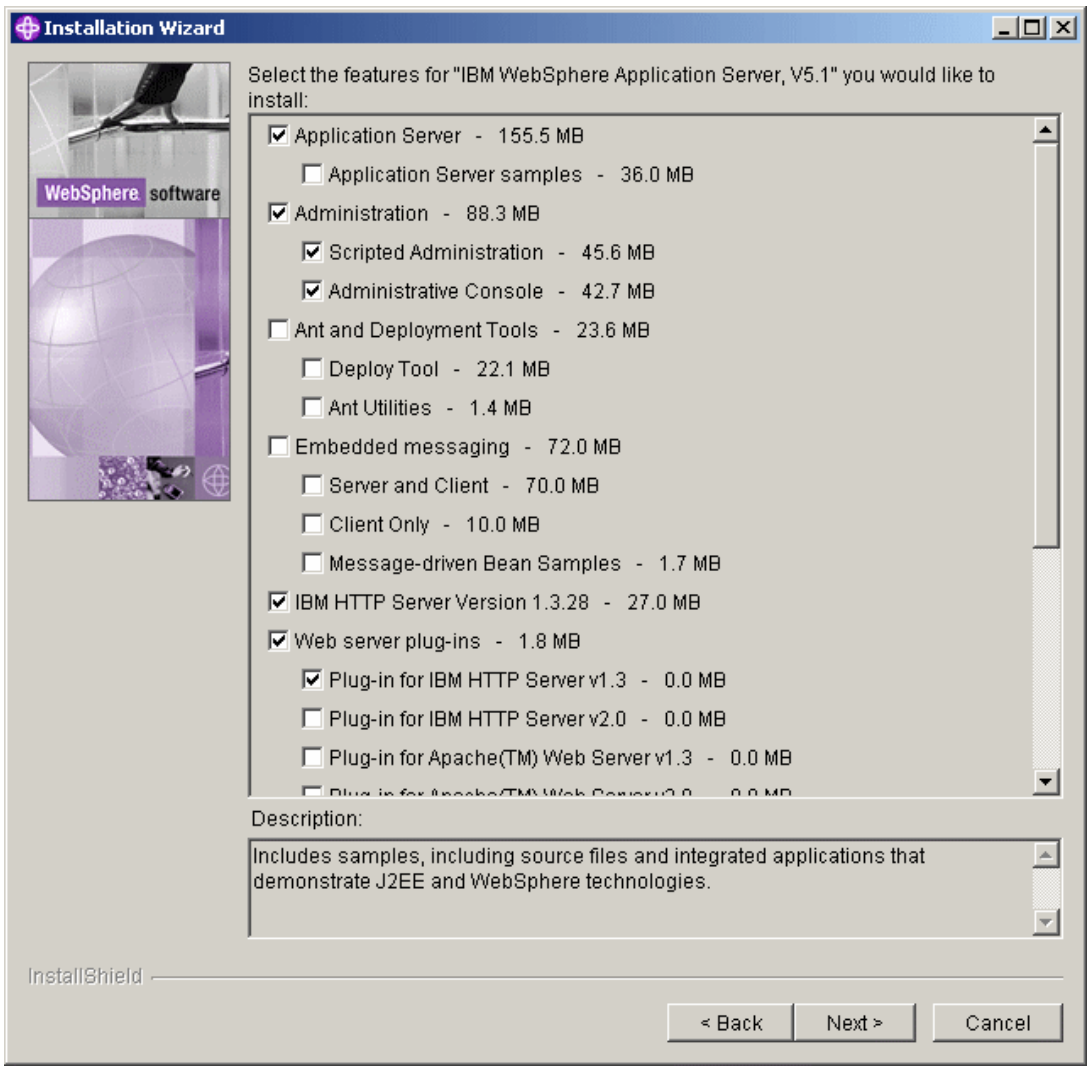

Installation Wizard
WebSphere software
Select the features for "IBM WebSphere Application Server, V5.1" you would like to install:
Application Server - 155.5 MB
Application Server samples - 36.0 MB
Administration - 88.3 MB
Scripted Administration - 45.6 MB
Administrative Console - 42.7 MB
Ant and Deployment Tools - 23.6 MB
Deploy Tool - 22.1 MB
Ant Utilities - 1.4 MB
Embedded messaging - 72.0 MB
Server and Client - 70.0 MB
Client Only - 10.0 MB
Message-driven Bean Samples - 1.7 MB
IBM HTTP Server Version 1.3.28 - 27.0 MB
Web server plug-ins - 1.8 MB
Plug-in for IBM HTTP Server v1.3 - 0.0 MB
Plug-in for IBM HTTP Server v2.0 - 0.0 MB
Plug-in for Apache(TM) Web Server v1.3 - 0.0 MB
Description:
Includes samples, including source files and integrated applications that demonstrate J2EE and WebSphere technologies.
InstallShield
< Back
Next >
Cancel

Figure 8-5 Component selection dialog

Important: If you have the Internet Information Server installed on the machine where you are performing WebSphere installation there may be a port conflict on port 80. To prevent this configure your World Wide Web Publishing Service not to start automatically, or even to the disabled state.

Downloaded from www.Manualslib.com manuals search engine

7. In the next window, shown in Figure 8-6, you may specify the directories where the software components will be installed. Leave the default values and click **Next**.

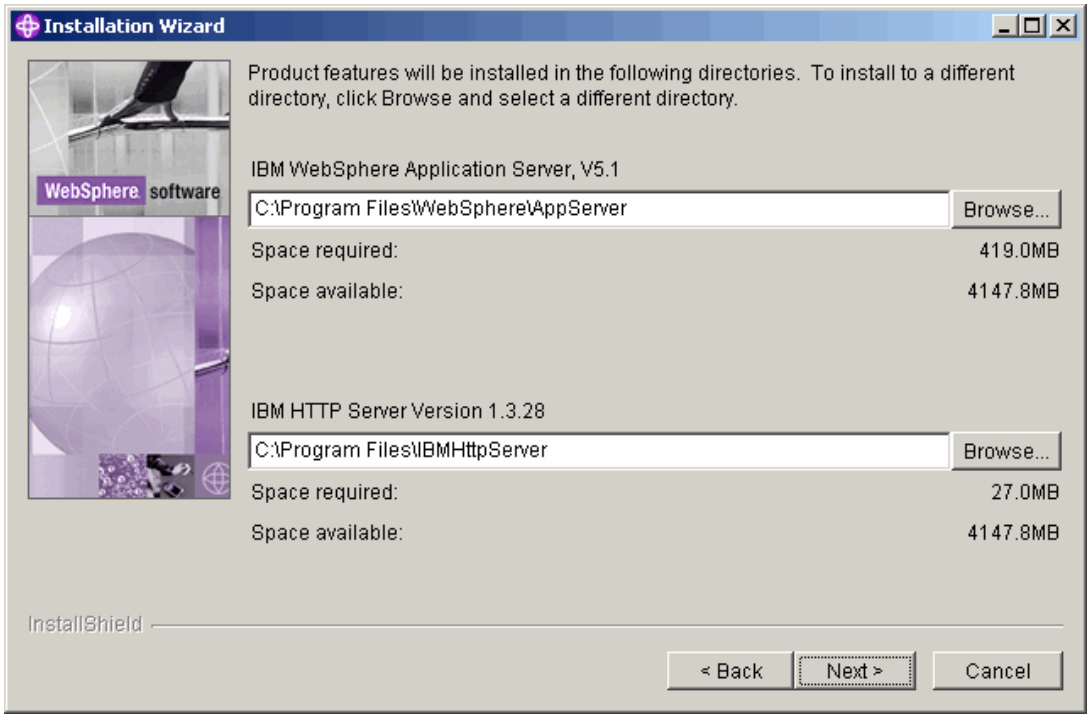


Figure 8-6 Destination folder selection window

Downloaded from www.Manualslib.com manuals search engine

8. In the next window you must specify the node name and host name for the Application Server to use. Both fields will be filled in with your server host name by default, as shown in Figure 8-7. We recommend that you leave the defaults and click **Next**.

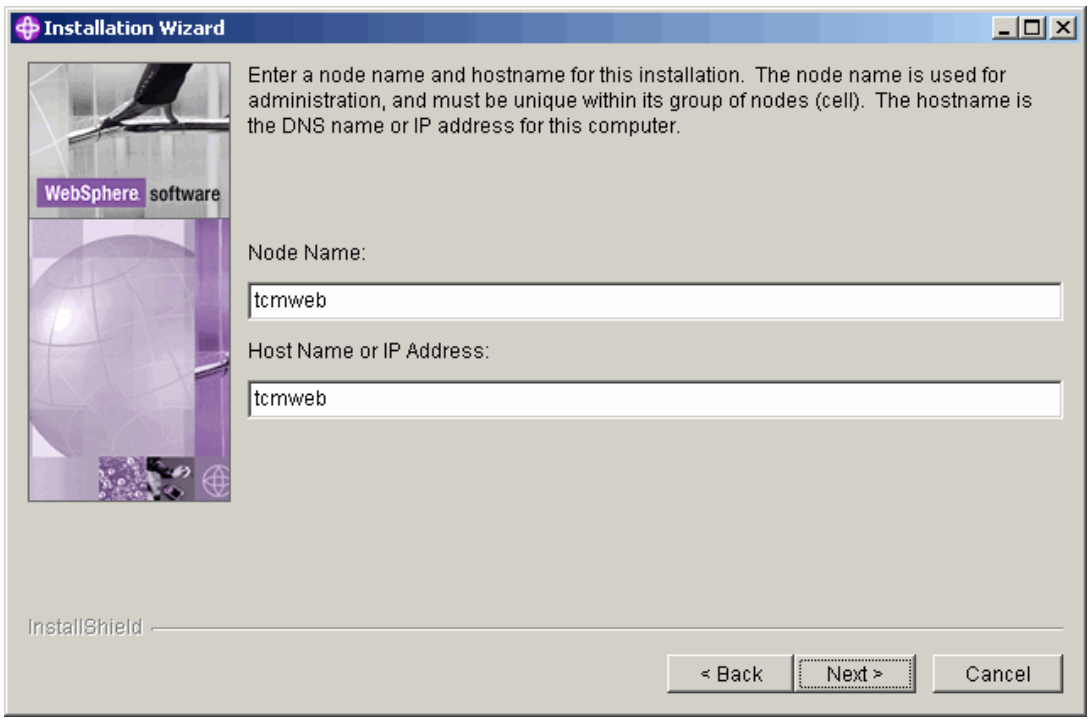

Installation Wizard
WebSphere software
Enter a node name and hostname for this installation. The node name is used for administration, and must be unique within its group of nodes (cell). The hostname is the DNS name or IP address for this computer.
Node Name:
tcmweb
Host Name or IP Address:
tcmweb
InstallShield
< Back
Next >
Cancel

Figure 8-7 Node name selection window

Downloaded from www.Manualslib.com manuals search engine

9. The next dialog (Figure 8-8) allows you to select whether you want your Web components to run as a service. To accept the default selection, which is yes for both components, enter a user name and password for the user account you want to use for the service to run. Check the WebSphere installation guide for the specific permissions required for this user. For our lab we decided to run the service using the administrator account. When you are done click **Next**.

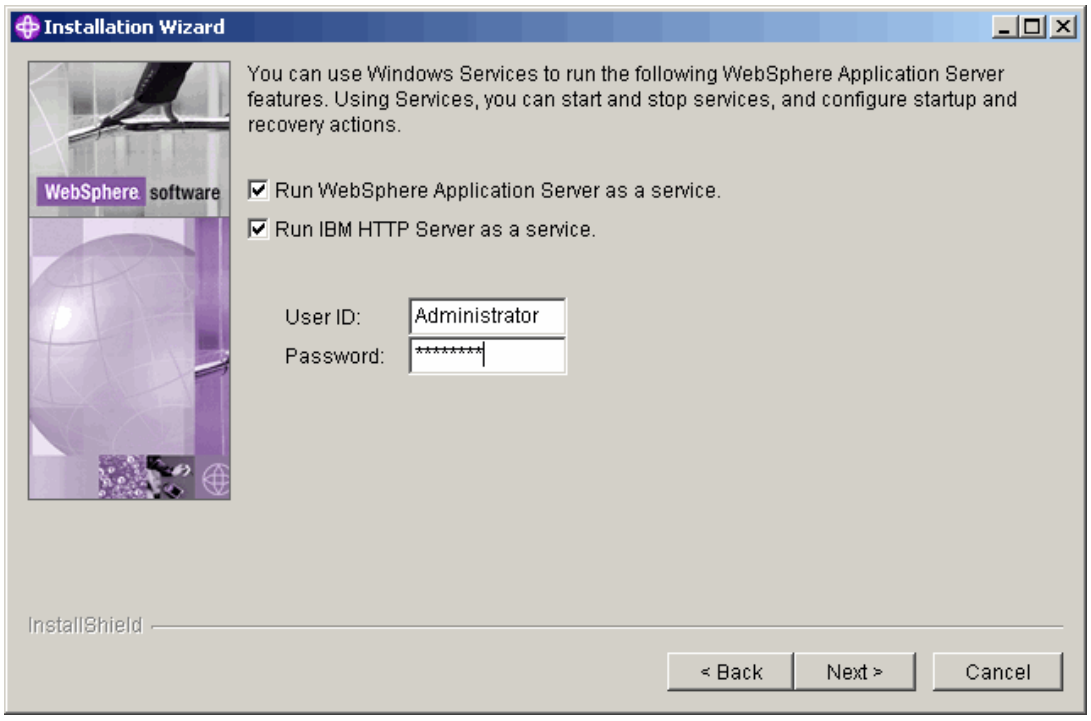

Installation Wizard
WebSphere software
You can use Windows Services to run the following WebSphere Application Server features. Using Services, you can start and stop services, and configure startup and recovery actions.
Run WebSphere Application Server as a service.
Run IBM HTTP Server as a service.
User ID:
Administrator
Password:
****
InstallShield
< Back
Next >
Cancel

Figure 8-8 Run as a service selection window

Downloaded from www.Manualslib.com manuals search engine

10. The next window presented to you contains the installation options summary, as shown in Figure 8-9. To proceed with the installation click **Next**.

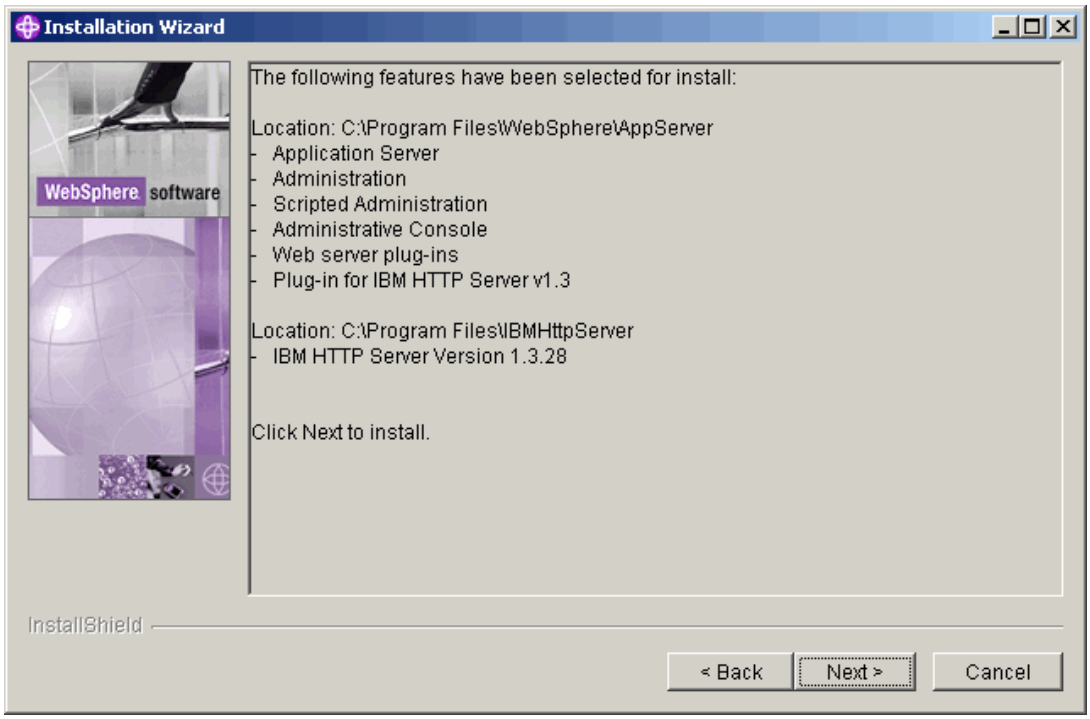


Figure 8-9 Installation options summary

11. The installation progress is shown in another dialog. The process has several phases:
    - Installation of WebSphere Application Server
    - Installation of IBM HTTP Server
    - Installation of three Web applications

Downloaded from www.Manualslib.com manuals search engine

It may take a few minutes to complete the installation. Then you are presented with the online registration window, as shown in Figure 8-10. Uncheck “Register this product now” and click **Next**.

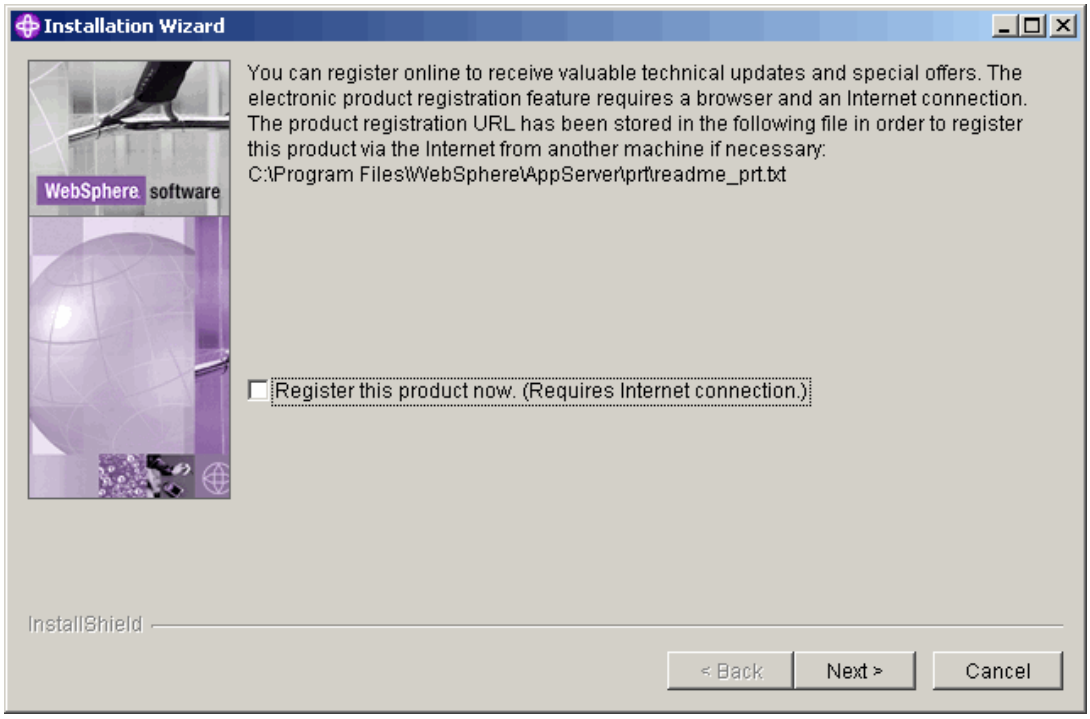

Installation Wizard
WebSphere software
You can register online to receive valuable technical updates and special offers. The electronic product registration feature requires a browser and an Internet connection. The product registration URL has been stored in the following file in order to register this product via the Internet from another machine if necessary:
C:\Program Files\WebSphere\AppServer\prt\readme_prt.txt
Register this product now. (Requires Internet connection.)
InstallShield
< Back
Next >
Cancel

Figure 8-10 Online registration dialog

Downloaded from www.Manualslib.com manuals search engine

12. Finally, there remain two open windows. One of them is the First Steps dialog you can just exit. The second one, shown in Figure 8-11, presents the Installation status summary. To close the wizard click **Finish**.

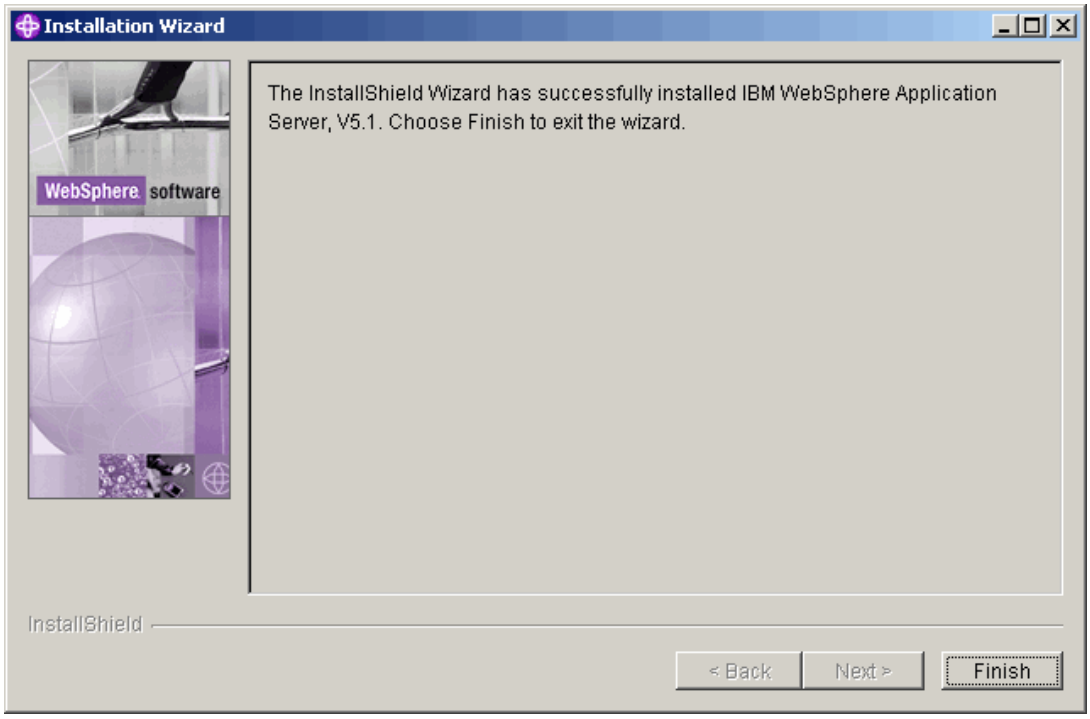

Installation Wizard
WebSphere software
The InstallShield Wizard has successfully installed IBM WebSphere Application Server, V5.1. Choose Finish to exit the wizard.
InstallShield
< Back
Next >
Finish

Figure 8-11 Installation status summary window

Now you are ready to update your environment with the latest fixes.

Patching WebSphere Application Server installation

The Tivoli Configuration Manager installation media set contains a CD with the base version of the WebSphere Application Server 5.1. Before installing further components you must install the latest recommended cumulative fix, which is 11 at the time we wrote this book. The procedure for installing the latest patches is:

1. Unpack the fix pack files downloaded from the network into a temporary local directory. You can use the same directory for both Fix Pack 1 and Cumulative Fix 11.
2. Open the command prompt. Go to the WebSphere bin directory, which is C:\Program Files\WebSphere\AppServer\bin by default. Stop the WebSphere Application Server server using the following command:

```
stopServer.bat server1
```


Downloaded from www.Manualslib.com manuals search engine

3. Make sure that the IBM HTTP server is not running (look for the Apache.exe or httpd processes). If it is running it can be stopped using the Services panel or with the following commands:

```
net stop "IBM HTTP Administration 1.3.28"
net stop "IBM HTTP Server 1.3.28"
```

4. Set up the proper environment variables using the following command:

```
cd C:\Program Files\WebSphere\AppServer\bin
SetupCmdLine.bat
```

5. Go to the temporary directory you have created in step 1 and start the Update installation wizard with the following command:

```
updateWizard.bat
```

6. Follow the wizard, ensuring that:

   a. The WebSphere Application Server installation path is properly recognized (should be C:\Program Files\WebSphere\AppServer, as shown in Figure 8-12).

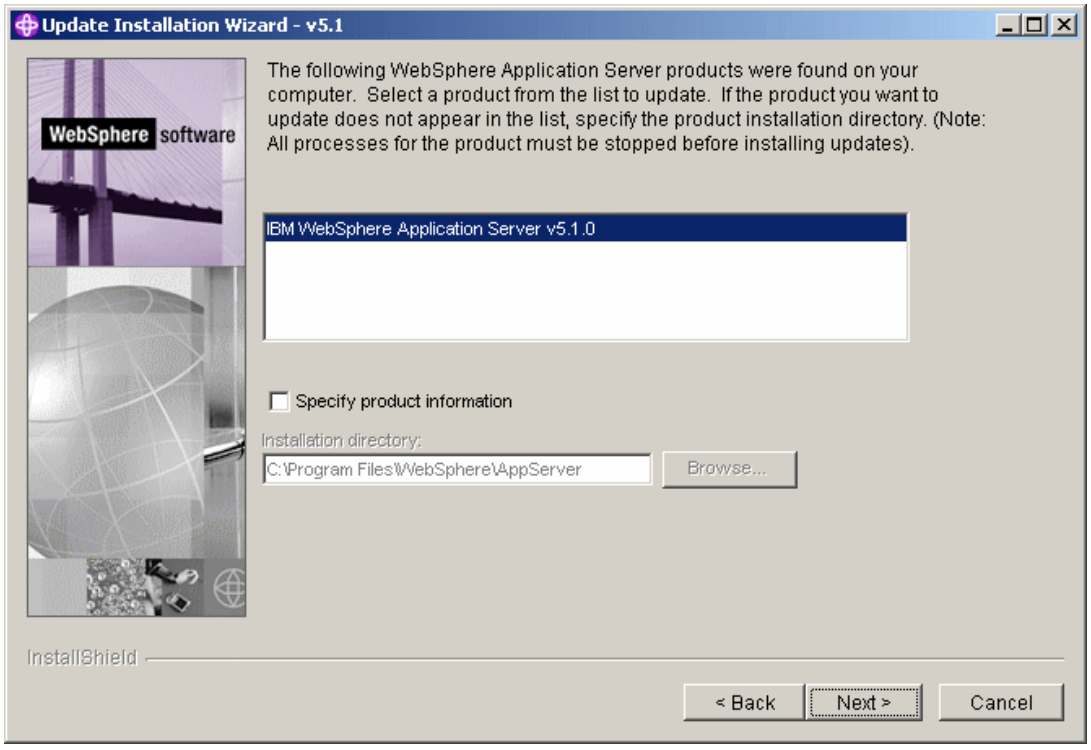

Update Installation Wizard - v5.1
WebSphere software
The following WebSphere Application Server products were found on your computer. Select a product from the list to update. If the product you want to update does not appear in the list, specify the product installation directory. (Note: All processes for the product must be stopped before installing updates).
IBM WebSphere Application Server v5.1.0
Specify product information
Installation directory:
C:\Program Files\WebSphere\AppServer
Browse...
InstallShield
< Back
Next >
Cancel

Figure 8-12 WebSphere product location

Downloaded from www.Manualslib.com manuals search engine

b. The Install fix packs option is selected, as shown in Figure 8-13.

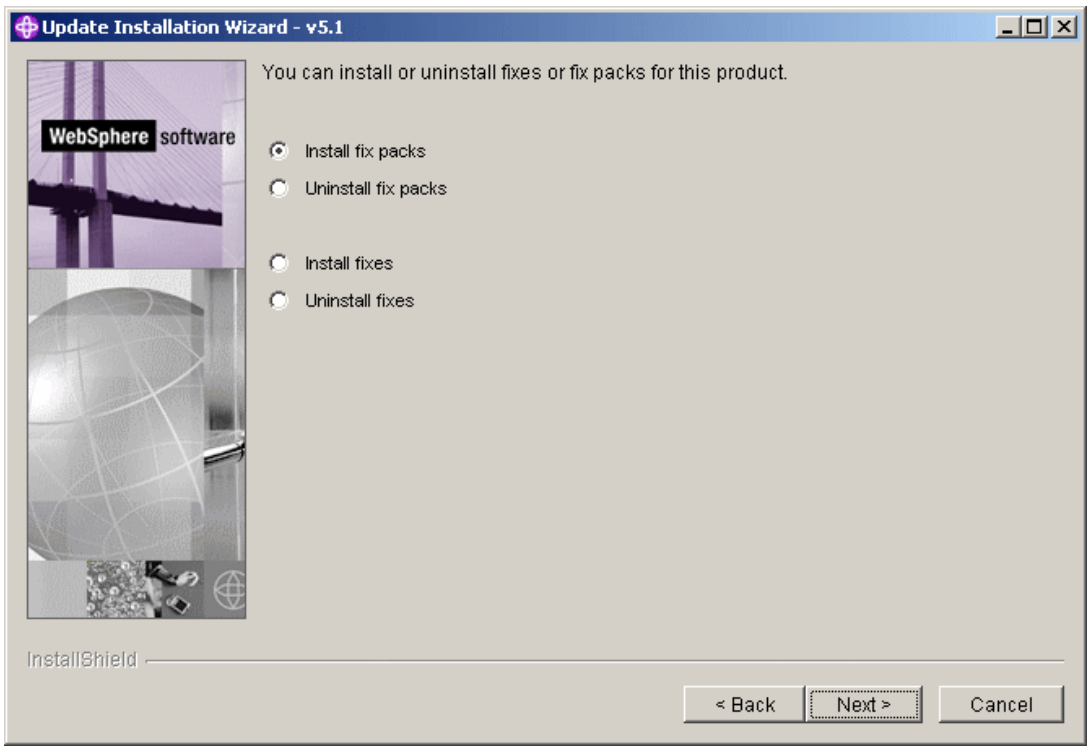


Figure 8-13 Installation option selection

Downloaded from www.Manualslib.com manuals search engine

c. The directory location provided for the fix packs is the fix packs subdirectory under your temporary directory you have created in step 1 (Figure 8-14).

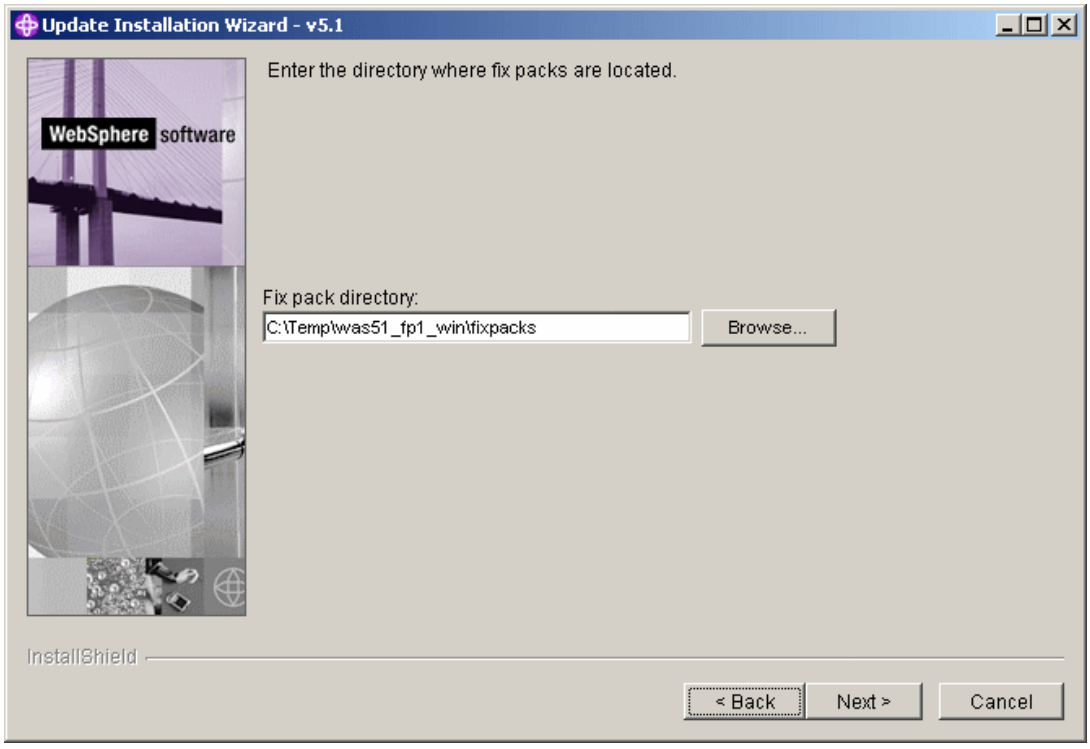


Figure 8-14 Fix packs directory location

7. As Fix Pack 1 is the prerequisite to Cumulative Fix 11, this second one will not show up in the list of available fix packs until the first one is installed. You must run the procedure twice, installing first Fix Pack 1 and then Cumulative Fix 11.

Creating the necessary user account

The Web Gateway component requires that a DB2 user exists on every system where the Web Gateway database is installed. The DB2 user (the default name is dmsadmin) owns the database tables in the Web Gateway database.

The correct group for the dmsadmin user is the DB2 administrator group ID, which is DB2ADMNS on Windows.

To create this user account issue as a administrative user the following commands:

```
net user dmsadmin <password> /add
net localgroup DB2ADMNS dmsadmin /add
```


Downloaded from www.Manualslib.com manuals search engine

Now you can continue with the Tivoli Configuration Manager Web Gateway installation.

Installation of Tivoli Configuration Manager Web Gateway

In this section we detail the steps for Tivoli Configuration Manager Web Gateway. To install this component you need the Tivoli Configuration Manager Web Gateway CD, which is included with your Tivoli Configuration Manager installation bundle.

1. Go to the directory with the installation media and start the installation by running the following command:

   ```
   setup.exe
   ```

2. In the Language Selection dialog (shown in Figure 8-15) leave the default selection (English) and click **OK**.

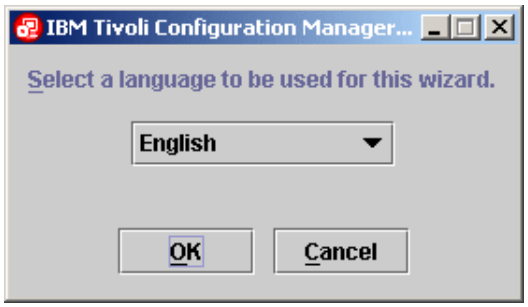


Figure 8-15 Language selection dialog

Downloaded from www.Manualslib.com manuals search engine

3. The welcome window is presented (Figure 8-16). Click **Next**.

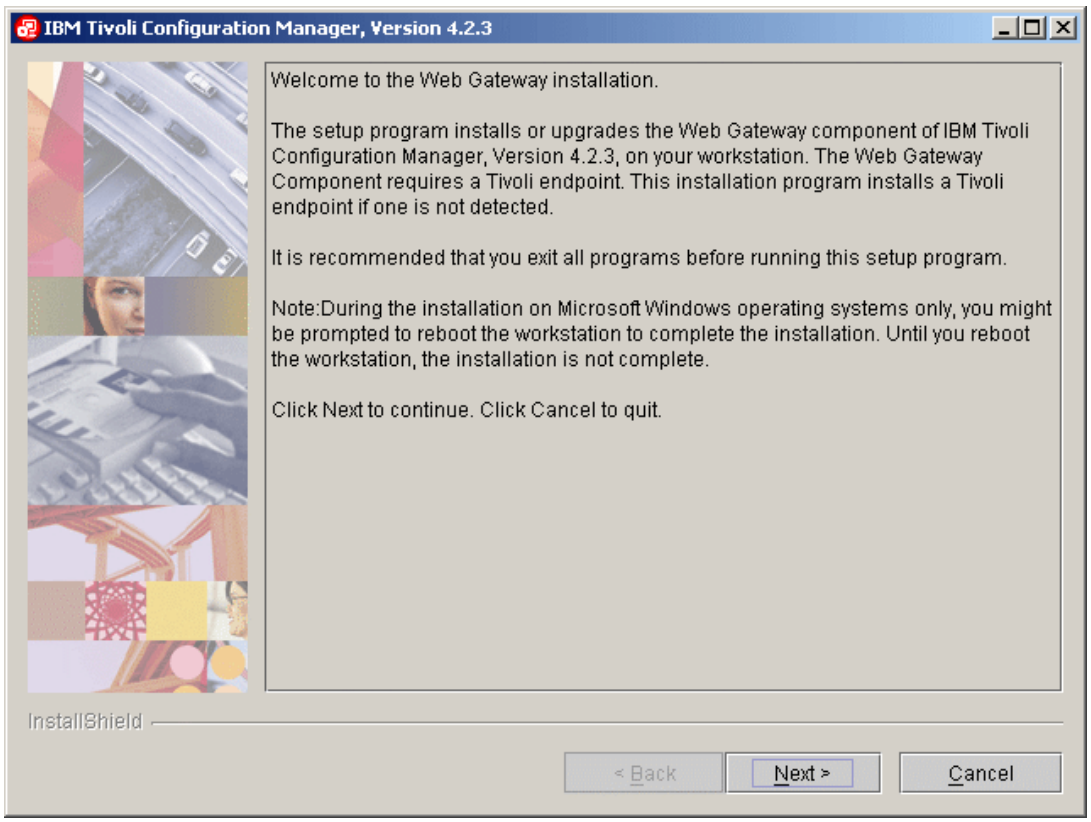

IBM Tivoli Configuration Manager, Version 4.2.3
Welcome to the Web Gateway installation.
The setup program installs or upgrades the Web Gateway component of IBM Tivoli Configuration Manager, Version 4.2.3, on your workstation. The Web Gateway Component requires a Tivoli endpoint. This installation program installs a Tivoli endpoint if one is not detected.
It is recommended that you exit all programs before running this setup program.
Note:During the installation on Microsoft Windows operating systems only, you might be prompted to reboot the workstation to complete the installation. Until you reboot the workstation, the installation is not complete.
Click Next to continue. Click Cancel to quit.
InstallShield
< Back
Next >
Cancel

Figure 8-16 Welcome window

Downloaded from www.Manualslib.com manuals search engine

4. In the next window (Figure 8-17), the standard license agreement is shown. Accept the license and click **Next**.

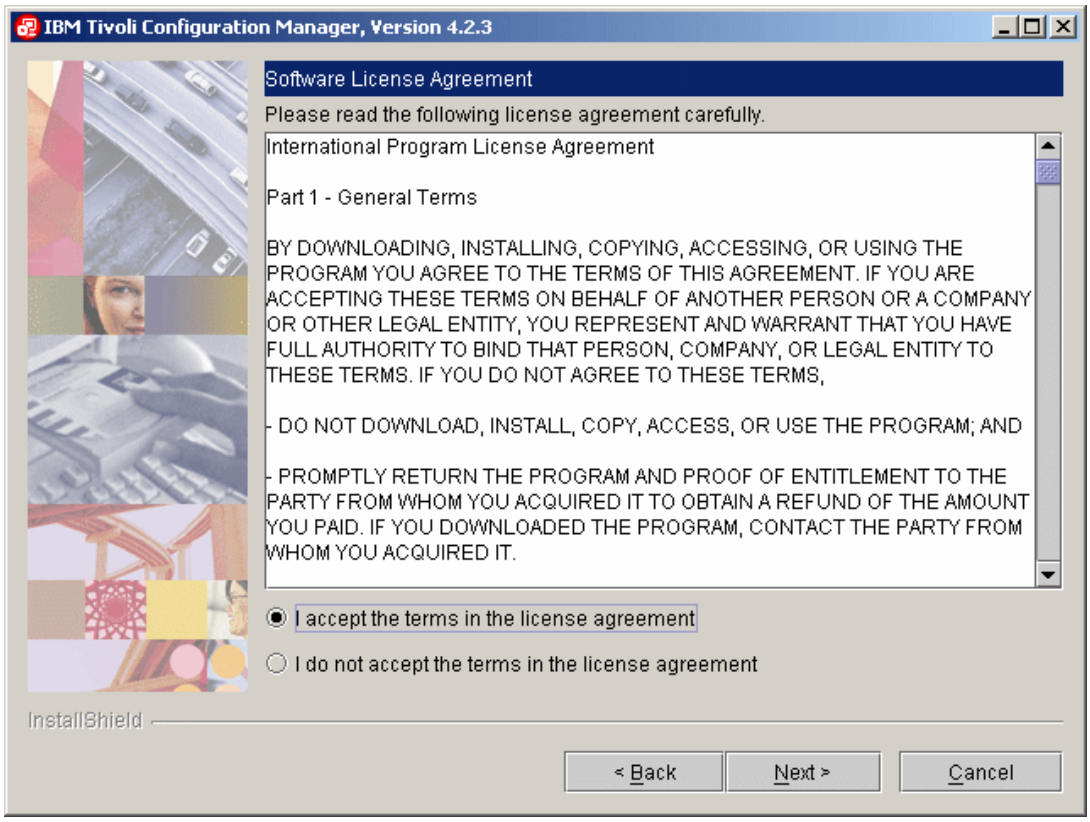

IBM Tivoli Configuration Manager, Version 4.2.3
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED IT TO OBTAIN A REFUND OF THE AMOUNT YOU PAID. IF YOU DOWNLOADED THE PROGRAM, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Figure 8-17 License agreement window

Downloaded from www.Manualslib.com manuals search engine

5. The component selection is displayed, as shown in Figure 8-18. Make sure that all three options are selected and click **Next**.

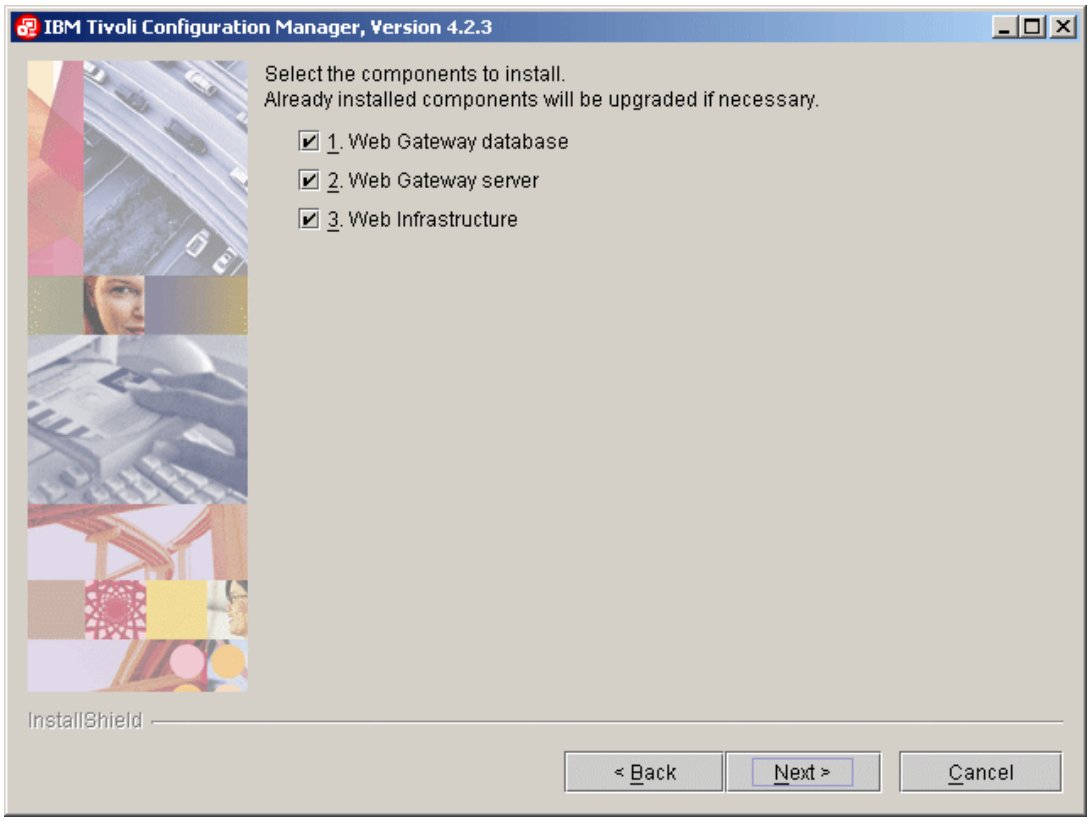

IBM Tivoli Configuration Manager, Version 4.2.3
Select the components to install.
Already installed components will be upgraded if necessary.
1. Web Gateway database
2. Web Gateway server
3. Web Infrastructure
InstallShield
< Back
Next >
Cancel

Figure 8-18 Component selection

Downloaded from www.Manualslib.com manuals search engine

6. The installation directory selection window is displayed (Figure 8-19). Accept the default path but make sure that the drive has at least 510 MB of free space and click **Next**.

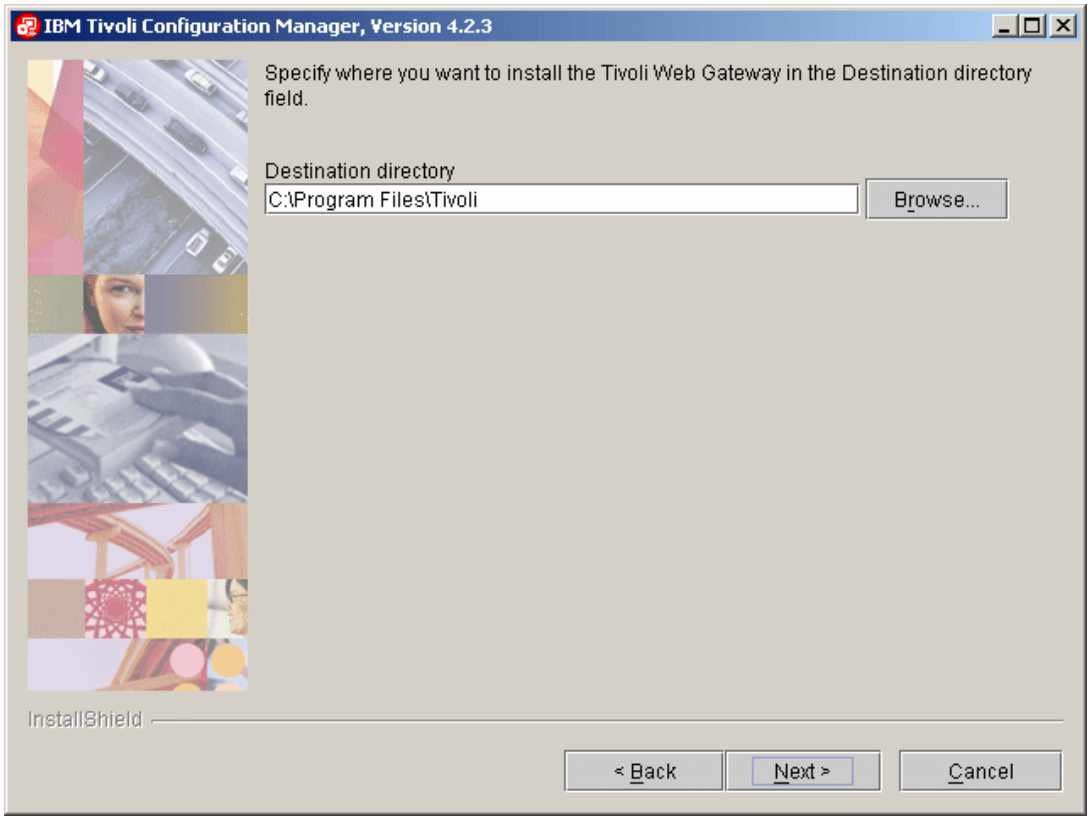

IBM Tivoli Configuration Manager, Version 4.2.3
Specify where you want to install the Tivoli Web Gateway in the Destination directory field.
Destination directory
C:\Program Files\Tivoli
Browse...
InstallShield
< Back
Next >
Cancel

Figure 8-19 Installation directory selection window

Downloaded from www.Manualslib.com manuals search engine

7. In the next dialog (Figure 8-20) most of the fields are already filled in. Provide the passwords for the DB2 administration user and the dmsadmin user you have created according to the procedure described in “Creating the necessary user account” on page 374 and click **Next**.

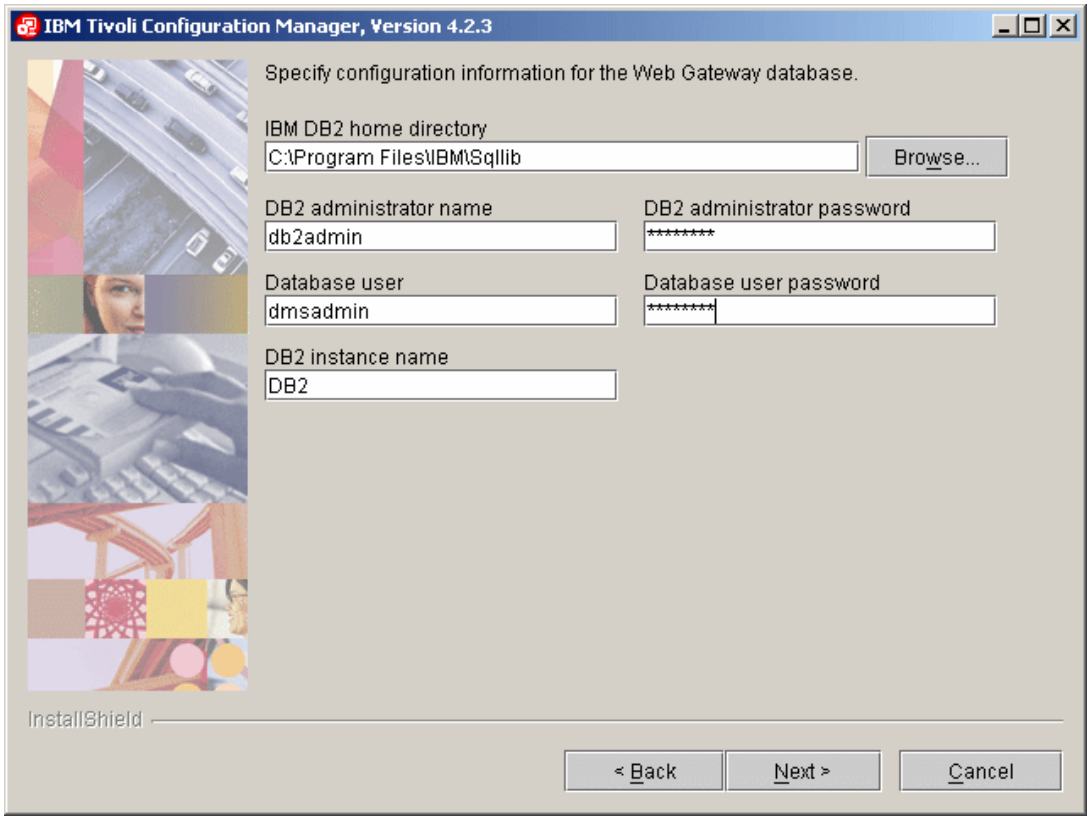


Figure 8-20 Database configuration window

Downloaded from www.Manualslib.com manuals search engine

8. The Web infrastructure configuration window is displayed (Figure 8-21). Check whether the right paths are entered (usually these are the defaults for the selected platform) and click **Next**.

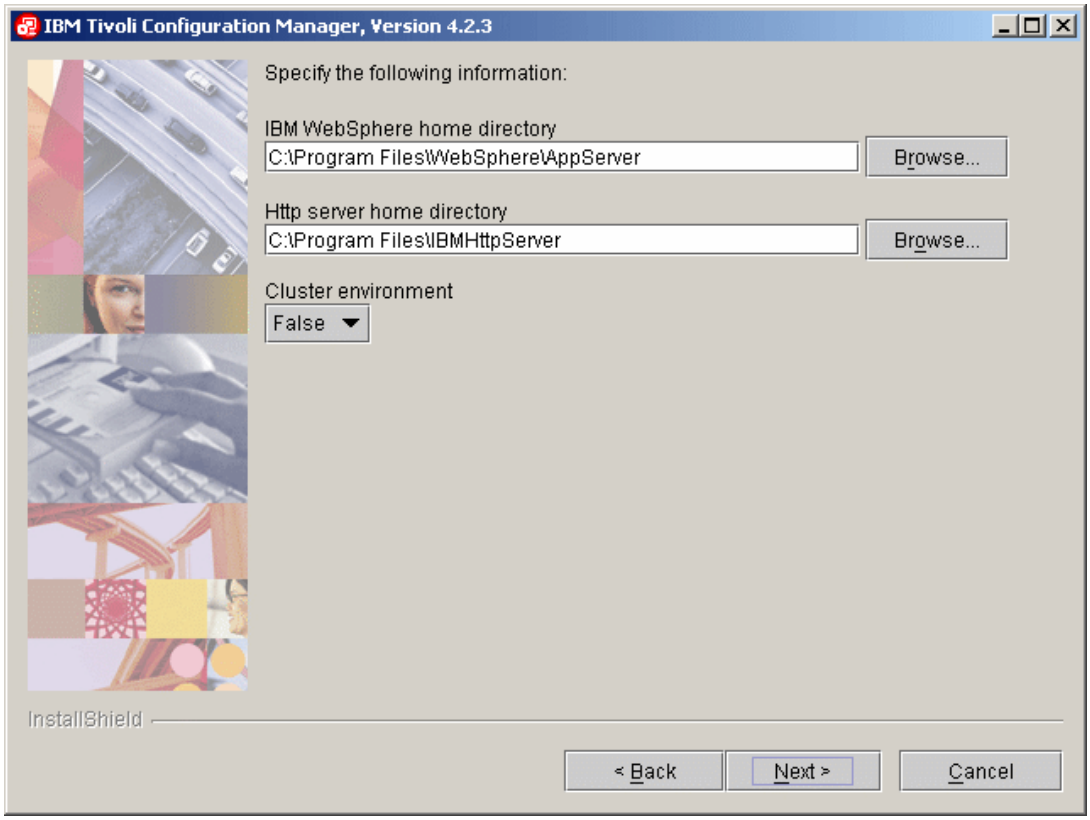


Figure 8-21 Web infrastructure configuration window

9. If there was no Tivoli Endpoint installed on the server, you are presented with the Endpoint configuration dialog. Leave the default installation path and ports and provide the additional option in the following form:

```
-g <gateway_address>+9494
```


Downloaded from www.Manualslib.com manuals search engine

If your Tivoli Configuration Manager is a single node installation this would be localhost, as shown in the Figure 8-22. Then click **Next**.

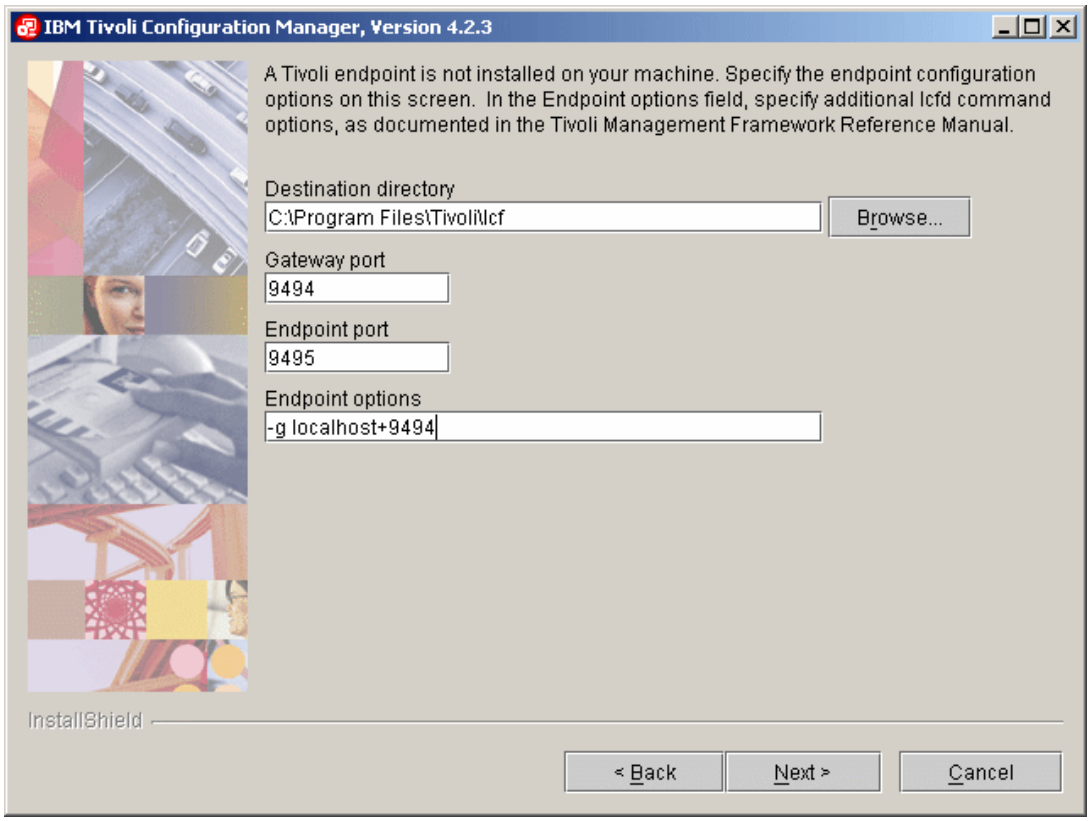

IBM Tivoli Configuration Manager, Version 4.2.3
A Tivoli endpoint is not installed on your machine. Specify the endpoint configuration options on this screen. In the Endpoint options field, specify additional lcfd command options, as documented in the Tivoli Management Framework Reference Manual.
Destination directory
C:\Program Files\Tivoli\lcf
Browse...
Gateway port
9494
Endpoint port
9495
Endpoint options
-g localhost+9494
InstallShield
< Back
Next >
Cancel

Figure 8-22 Endpoint configuration window

Downloaded from www.Manualslib.com manuals search engine

10. The Secure access configuration window is presented, as shown in Figure 8-23. Since we are not using Tivoli Access Manager in our environment accept the default (*Enable security* is *False*) and click **Next**.

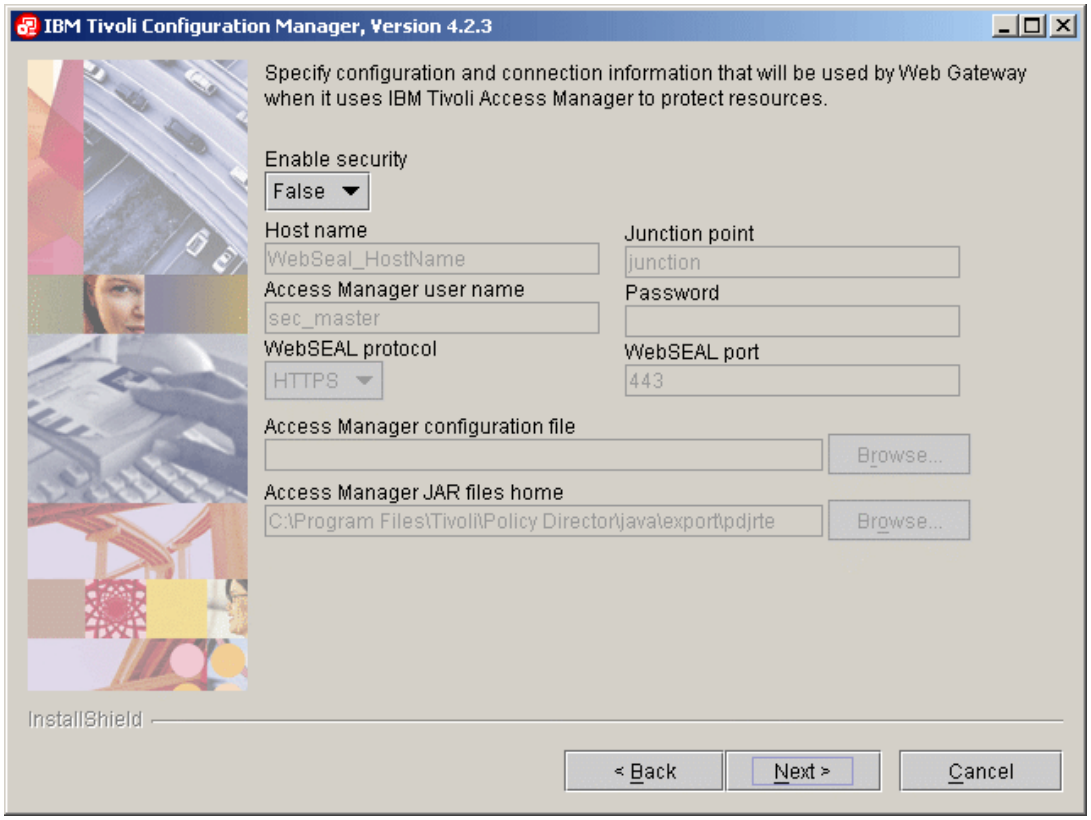


Figure 8-23 Secure access configuration

Downloaded from www.Manualslib.com manuals search engine

11. The summary of the selected installation options is presented, as shown in Figure 8-24. Click **Next** to proceed with the installation.

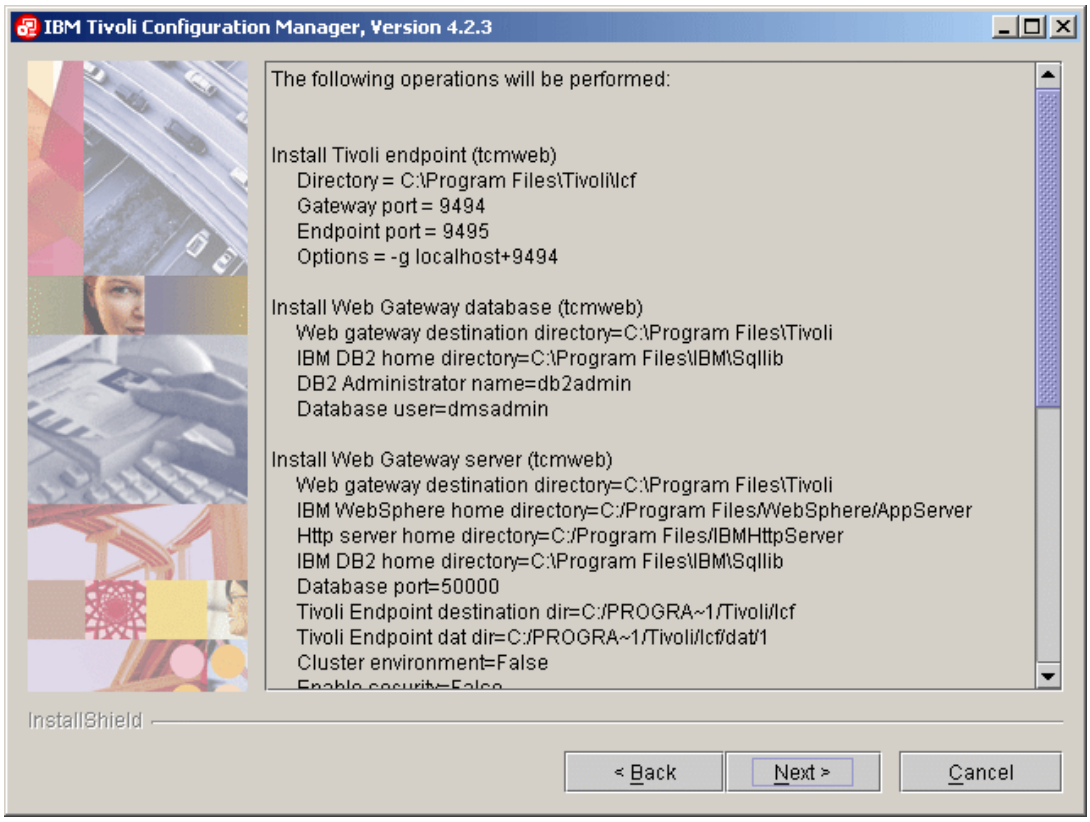

IBM Tivoli Configuration Manager, Version 4.2.3
The following operations will be performed:
Install Tivoli endpoint (tcmweb)
Directory = C:\Program Files\Tivoli\lcf
Gateway port = 9494
Endpoint port = 9495
Options = -g localhost+9494
Install Web Gateway database (tcmweb)
Web gateway destination directory=C:\Program Files\Tivoli
IBM DB2 home directory=C:\Program Files\IBM\SqlIib
DB2 Administrator name=db2admin
Database user=dmsadmin
Install Web Gateway server (tcmweb)
Web gateway destination directory=C:\Program Files\Tivoli
IBM WebSphere home directory=C:/Program Files/WebSphere/AppServer
Http server home directory=C:/Program Files/IBMHttpServer
IBM DB2 home directory=C:\Program Files\IBM\SqlIib
Database port=50000
Tivoli Endpoint destination dir=C:/PROGRA~1/Tivoli/lcf
Tivoli Endpoint dat dir=C:/PROGRA~1/Tivoli/lcf/dat/1
Cluster environment=False
InstallShield
< Back
Next >
Cancel

Figure 8-24 Summary of installation options

Downloaded from www.Manualslib.com manuals search engine

12. The installation can take a while depending on the configuration of your system. You can follow the progress of the installation in the dialog window. Figure 8-25 shows the final status. To finish the Web Gateway installation click **Finish**.

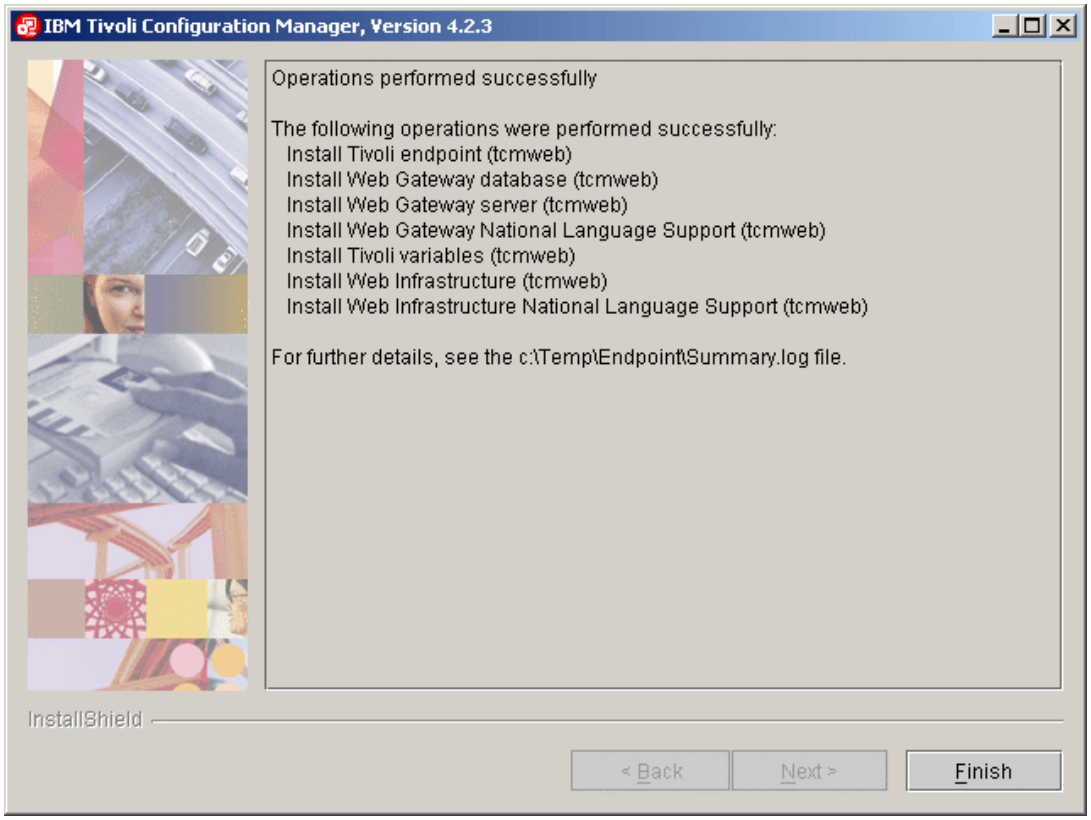

IBM Tivoli Configuration Manager, Version 4.2.3
Operations performed successfully
The following operations were performed successfully:
Install Tivoli endpoint (tcmweb)
Install Web Gateway database (tcmweb)
Install Web Gateway server (tcmweb)
Install Web Gateway National Language Support (tcmweb)
Install Tivoli variables (tcmweb)
Install Web Infrastructure (tcmweb)
Install Web Infrastructure National Language Support (tcmweb)
For further details, see the c:\Temp\Endpoint\Summary.log file.
InstallShield
< Back
Next >
Finish

Figure 8-25 Installation status window

Now that all of the prerequisites are installed and configured, you can proceed with the remediation server configuration.

After the Tivoli Configuration Manager Web Gateway installation there are two additional instances of WebSphere Application Server created. If everything worked fine you should have the following instances:

- server1
- DMS_AppServer
- WebUI_AppServer

8.2.3 Configuration of the remediation server

To successfully implement the solution an additional component is needed — the *Software Package Web Server*. It provides the interface between the remediation

Downloaded from www.Manualslib.com manuals search engine

handler located on the workstation attempting to connect to the network and the Tivoli Configuration Manager Web Gateway. The Software Package Web Server code is located in the *IISSCN Extension Pack2 for Tivoli Configuration Manager* file posted on the IBM Web page, as described in “Preparing for the installation” on page 360, and must be deployed into the WebSphere Application Server.

Installation of Software Package Web Server

In the steps below we describe how to install the Software Package Web Server. This procedure is also described in the *IISSCN: Tivoli Configuration Manager Extension Pack Quick Start Guide* included in the IISSCN Extension Start Guide (TCM) package.

1. Create a temporary directory on the Tivoli Configuration Manager Web Gateway server and extract the files from the *IISSCN Extension Pack2 for Tivoli Configuration Manager* file (iisscn_extension_pack2.zip) to this directory. The following files are included:

   – SoftwarePackageServer.ear
   – com.ibm.scm.nac.tcmremed.client.TCMRemed.jar
   – nac.win.any.hotfix.PostureHotfixV2.jar
   – nac.win.any.nav.PostureNavV2.jar
   – nac.win.any.netaccounts.PostureNetAccountsV2.jar
   – nac.win.any.oslevel.PostureOSLevelV2.jar
   – nac.win.any.regkey.PostureRegKeyV2.jar
   – nac.win.any.services.PostureServices.jar
   – tcmremed.tar

   A few additional files are located in the sample_policies subdirectory.

   – IISSCN_TCM_v2.00_win2000.pol
   – IISSCN_TCM_v2.00_winXP.pol
   – TCMCLI.pol

   For the next step the important file is SoftwarePackageServer.ear.

2. Start the WebSphere administrative console by opening the Web browser and pointing it to http://<tcm_web_gateway_server>:9090/admin.

Downloaded from www.Manualslib.com manuals search engine

3. If you have followed the installation of WebSphere Application Server as described in this book you should have no security turned on and you will see the standard login screen, as shown in Figure 8-26. Enter any name and click **OK**.

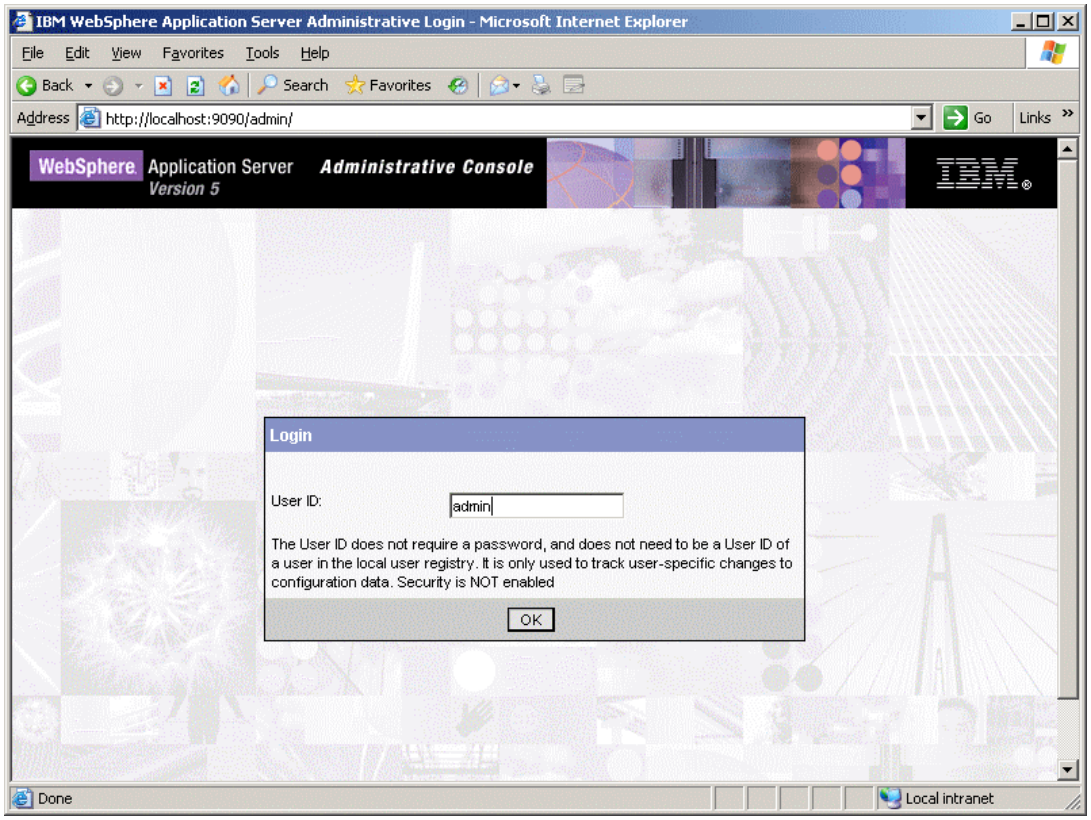

IBM WebSphere Application Server Administrative Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:9090/admin/
Go Links
WebSphere Application Server Version 5
Administrative Console
IBM
Login
User ID:
admin
The User ID does not require a password, and does not need to be a User ID of a user in the local user registry. It is only used to track user-specific changes to configuration data. Security is NOT enabled
OK
Done
Local intranet

Figure 8-26 WebSphere administrative console login

Downloaded from www.Manualslib.com manuals search engine

4. On the next page expand the **Applications** menu item in the left pane and click the **Install New Application** option. The new content should be displayed in the right pane, as shown in Figure 8-27.

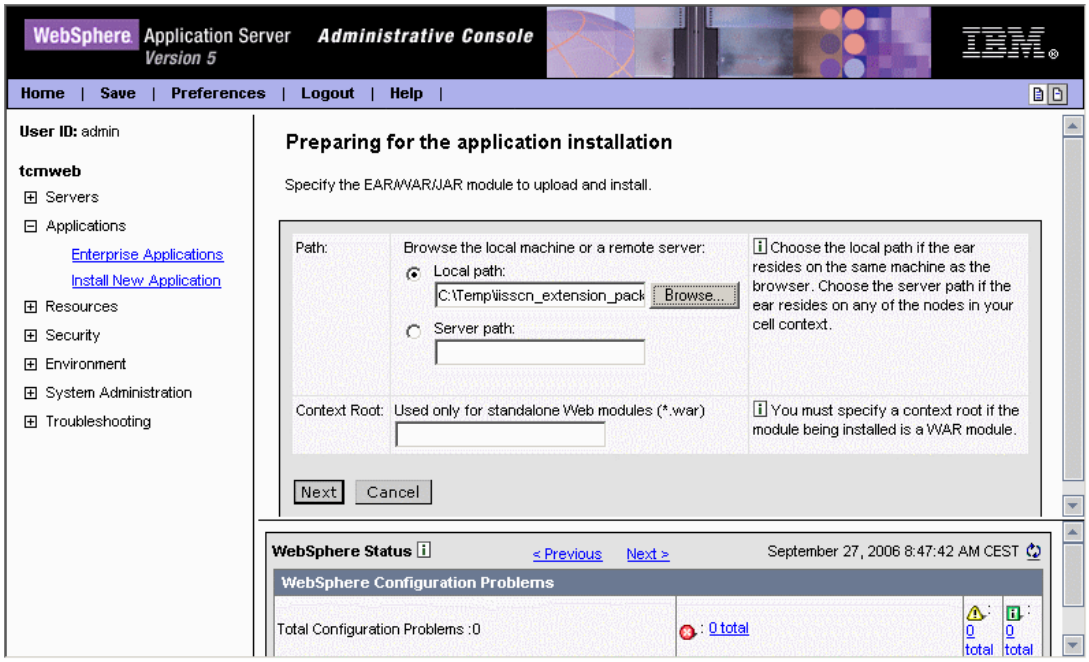


Figure 8-27 Install new application

5. In the Local path field enter the path to the SoftwarePackageServer.ear file located in the temporary directory created in step 1 and click **Next**.

Downloaded from www.Manualslib.com manuals search engine

6. The Preparing for the application installation window is displayed (Figure 8-28). Accept the defaults and click **Next**.

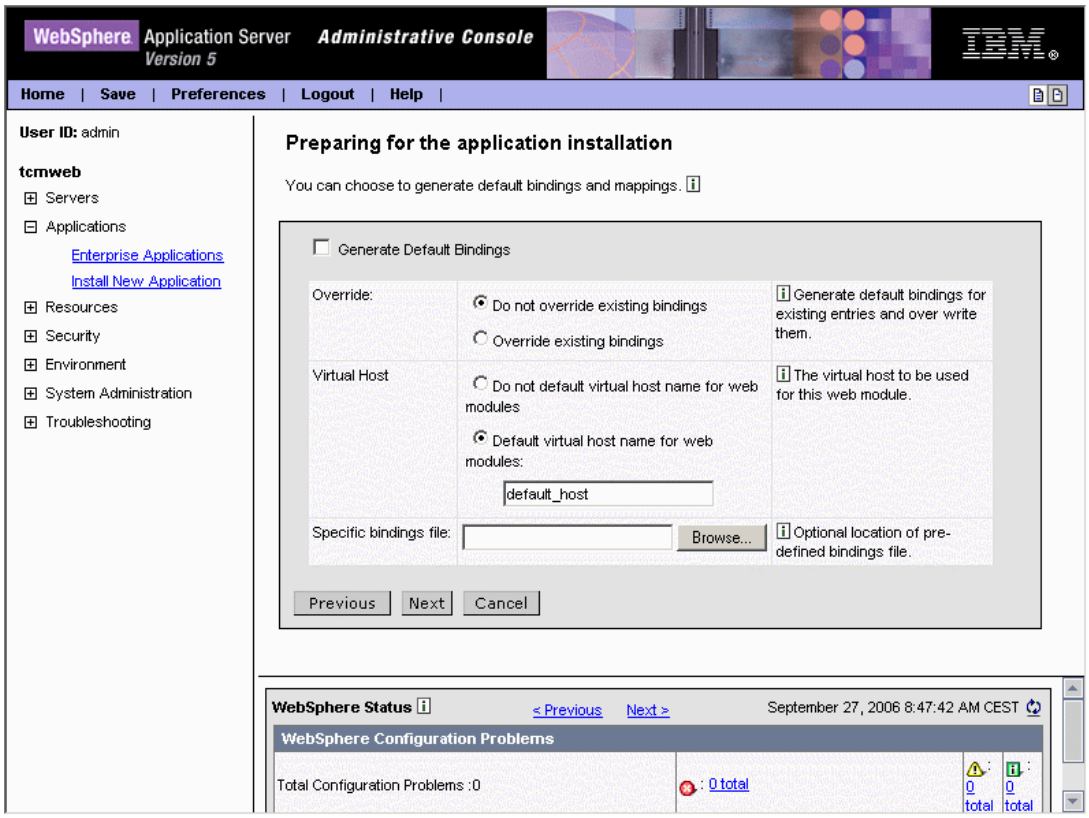


Figure 8-28 Preparing for the application installation

Downloaded from www.Manualslib.com manuals search engine

7. Leave the defaults and click **Next** in the several next windows until you reach the one shown in the Figure 8-29. Click **Finish** to start the actual installation. The button may be hidden in the lower part of the window, depending on the resolution of your display. In this case scroll down using the scroll bar on the right.

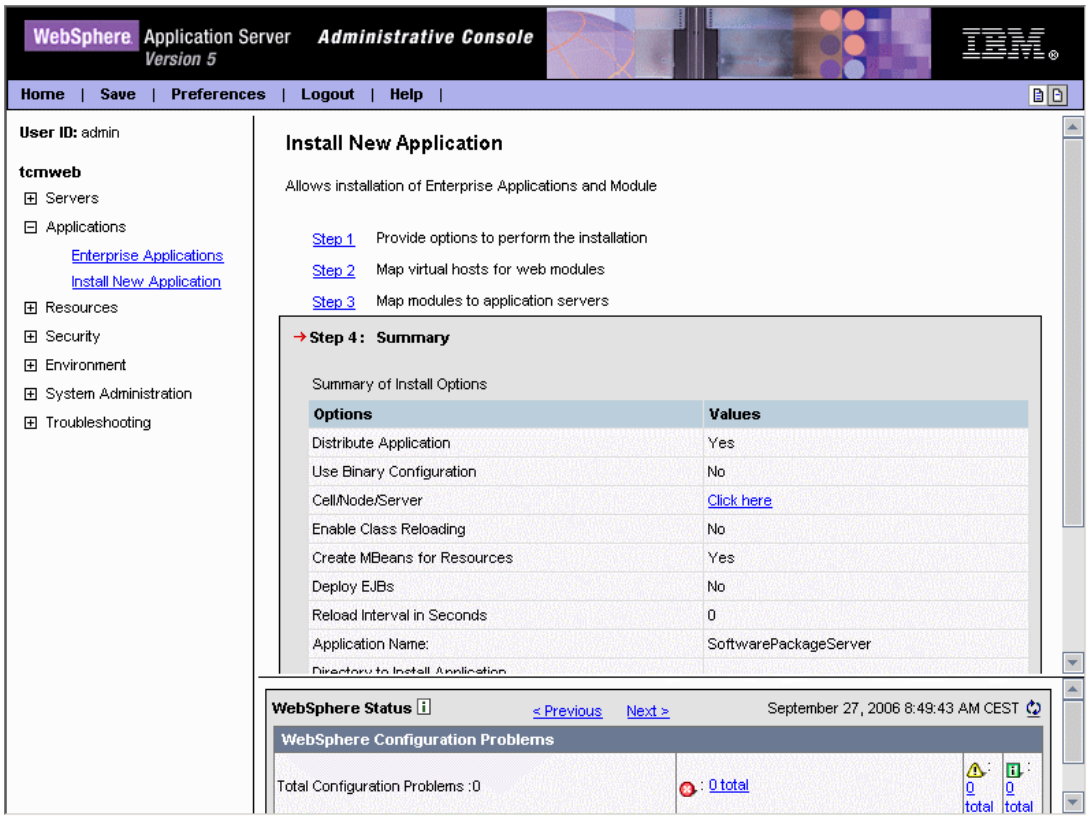


Figure 8-29 Installation option summary dialog

Downloaded from www.Manualslib.com manuals search engine

8. The installation may take a few seconds or few minutes depending on your server configuration. In the window that displays the installation results, find and click the **Save to Master Configuration** link.

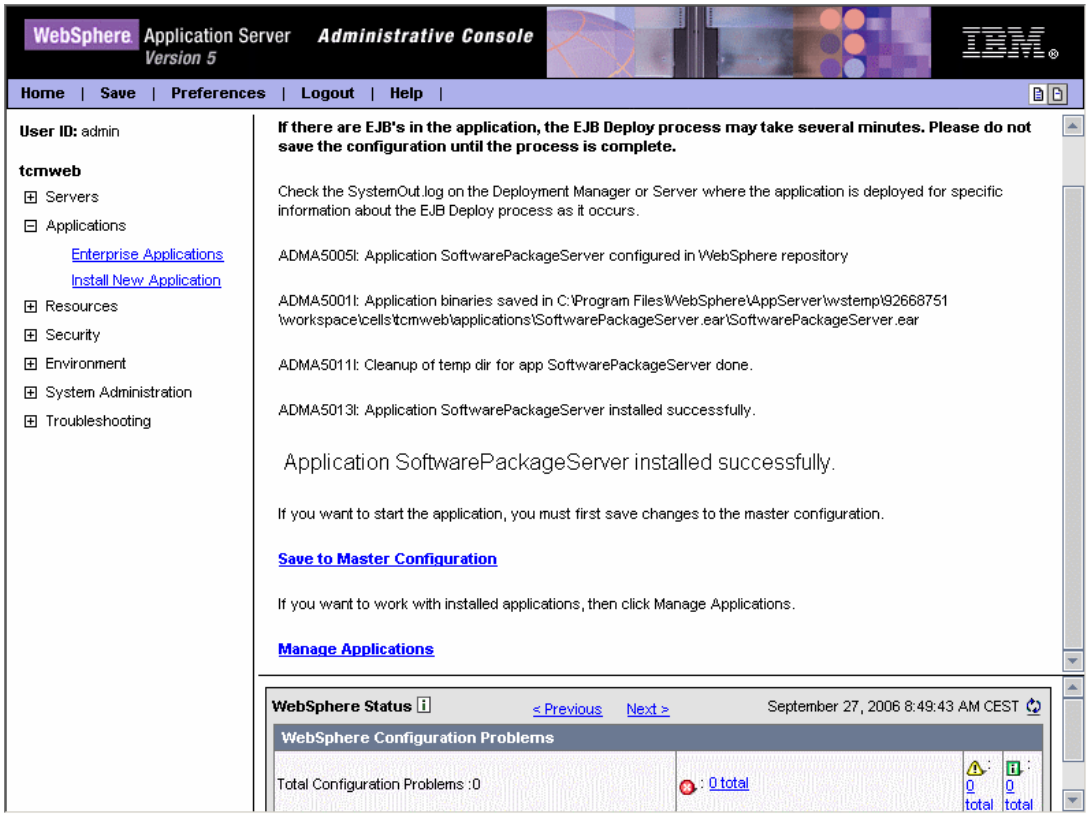

WebSphere Application Server Version 5
Administrative Console
IBM
Home | Save | Preferences | Logout | Help |
User ID: admin
tcmweb
Servers
Applications
Enterprise Applications
Install New Application
Resources
Security
Environment
System Administration
Troubleshooting
If there are EJB's in the application, the EJB Deploy process may take several minutes. Please do not save the configuration until the process is complete.
Check the SystemOut.log on the Deployment Manager or Server where the application is deployed for specific information about the EJB Deploy process as it occurs.
ADMA5005I: Application SoftwarePackageServer configured in WebSphere repository
ADMA5001I: Application binaries saved in C:\Program Files\WebSphere\AppServer\wstemp\92668751\workspace\cells\tcmweb\applications\SoftwarePackageServer.ear\SoftwarePackageServer.ear
ADMA5011I: Cleanup of temp dir for app SoftwarePackageServer done.
ADMA5013I: Application SoftwarePackageServer installed successfully.
Application SoftwarePackageServer installed successfully.
If you want to start the application, you must first save changes to the master configuration.
Save to Master Configuration
If you want to work with installed applications, then click Manage Applications.
Manage Applications
WebSphere Status
< Previous
Next >
September 27, 2006 8:49:43 AM CEST
WebSphere Configuration Problems
Total Configuration Problems :0
0 total
0 total
0 total

Figure 8-30 Installation status window

Downloaded from www.Manualslib.com manuals search engine

9. In the next window, shown in Figure 8-31, select **Save** to save the configuration changes to the master configuration file.

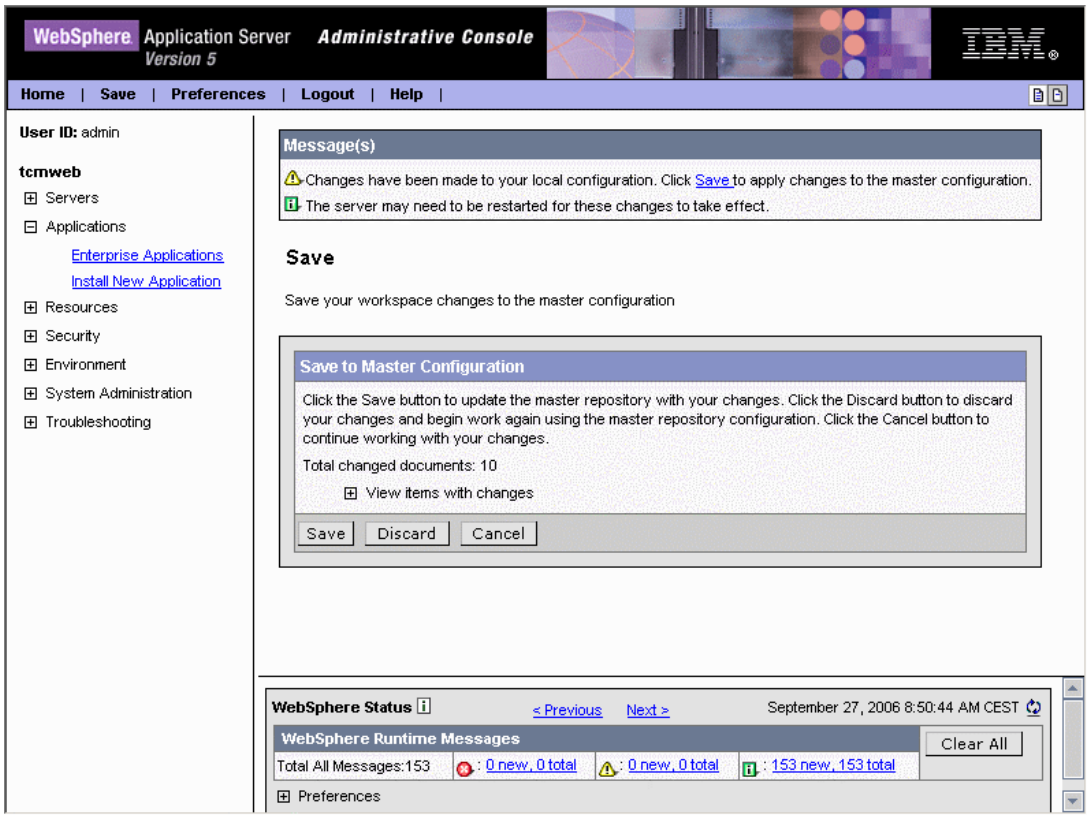

WebSphere Application Server Version 5
Administrative Console
IBM
Home | Save | Preferences | Logout | Help |
User ID: admin
tcmweb
Servers
Applications
Enterprise Applications
Install New Application
Resources
Security
Environment
System Administration
Troubleshooting
Message(s)
Changes have been made to your local configuration. Click Save to apply changes to the master configuration.
The server may need to be restarted for these changes to take effect.
Save
Save your workspace changes to the master configuration
Save to Master Configuration
Click the Save button to update the master repository with your changes. Click the Discard button to discard your changes and begin work again using the master repository configuration. Click the Cancel button to continue working with your changes.
Total changed documents: 10
View items with changes
Save
Discard
Cancel
WebSphere Status
< Previous
Next >
September 27, 2006 8:50:44 AM CEST
WebSphere Runtime Messages
Clear All
Total All Messages:153
0 new, 0 total
0 new, 0 total
153 new, 153 total
Preferences

Figure 8-31 Saving the configuration changes

Downloaded from www.Manualslib.com manuals search engine

10. When you click the **Enterprise Application** link under Applications in the left pane you should see a window similar to the one presented in Figure 8-32.

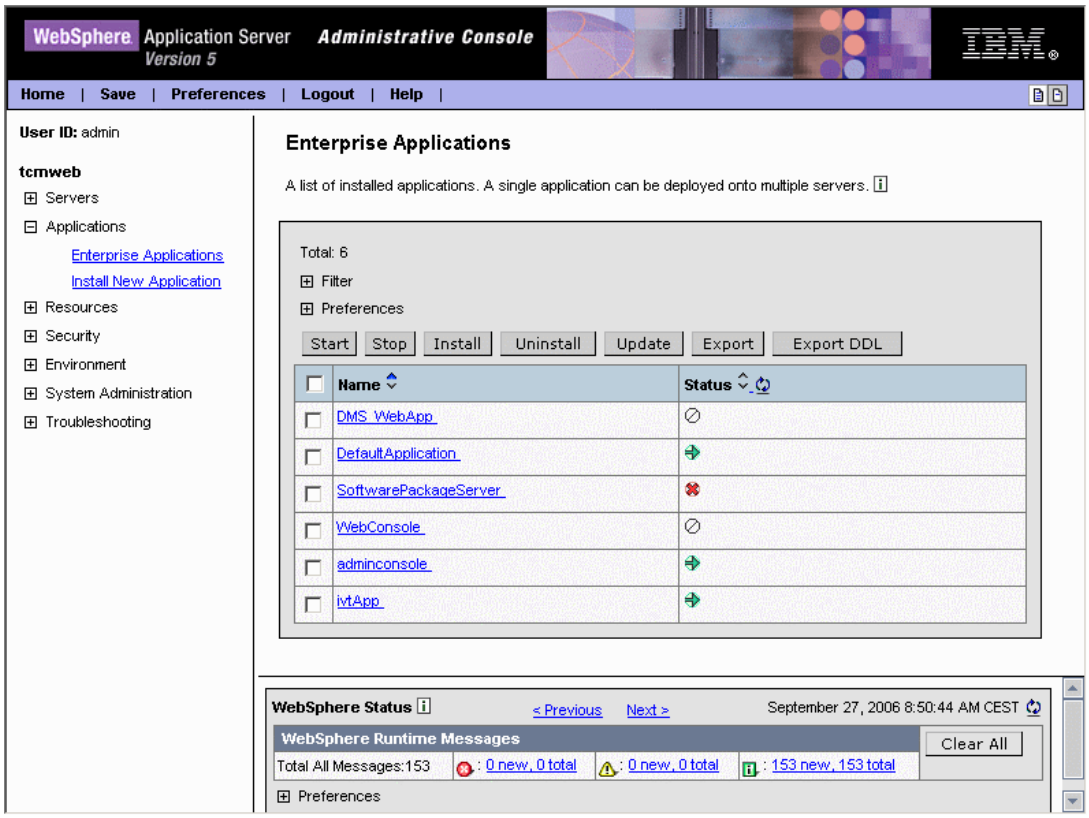


Figure 8-32 Enterprise Applications window

Configuration of the Software Package Web Server

The steps necessary to properly configure the Software Package Web Server are:

1. Create the a directory using the following commands:

   ```
   mkdir C:\Program Files\WebSphere\AppServer\installedApps\<your_server_name>
   \SoftwarePackageServer.ear\SoftwarePackageServerWeb.war\WEB-INF\lib
   ```

   Copy the file twguserpull.jar located in WebSphere home directory under the WebConsole.ear application directory into your new directory. This will be in the following directory:

   ```
   C:\Program Files\WebSphere\AppServer\installedApps\<your_server_name>\WebCo
   nsole.ear\WebUI.war\WEB-INF\lib\twguserpull.jar
   ```

2. Locate the twgConfig.properties file located in the directory:

   ```
   C:\Program Files\WebSphere\AppServer\installedApps\<your_server_name>\DMS_W
   ebApp.ear/twgserver.war/WEB-INF/classes/twgConfig.properties
   ```


Downloaded from www.Manualslib.com manuals search engine

Open the file using a text editor, and find the value of the WEB_SERVER_DOC_ROOT key in the file. In our lab this is:

```
C:\Program Files\IBMHttpServer\htdocs\en_US
```

3. Open the SoftwarePackageServerConfig.properties file located in the following directory using a text editor:

   ```
   C:\Program Files\WebSphere\AppServer\installedApps\<your_server_name>\Softw
   arePackageServer.ear\SoftwarePackageServerWeb.war\WEB-INF\classes
   ```

   Find the SPBBaseDirectory key in that file and replace its value with the value extracted in step 2. Save the modified file.

4. Finally restart the WebSphere Application server with the following commands:

   ```
   cd C:\Program Files\WebSphere\AppServer\bin
   stopServer.bat server1
   startServer.bat server1
   ```

This ends the installation and configuration of the remediation server itself. In the next section we describe the installation and configuration of the remediation workflows, used to automatically remediate noncompliant workstations.

8.2.4 Installation of the Software Package Utilities

The *IISSCN extension pack2 for Tivoli Configuration Manager* contains some sample remediation workflow definitions and utilities that can be helpful with creating the remediation workflows for the compliance policies defined on the Tivoli Security Compliance Manager Server. These utilities are located in the tcmremed.tar file. To set them up:

1. Open a command prompt and set up the environment variables for the Tivoli Management framework. Use the following command:

   ```
   cmd.exe /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
   ```

2. Change the working directory to the %BINDIR% and issue the following command:

   ```
   tar xvf <path_to_the_tcmremed.tar>
   ```

3. Configure the WorkflowPostureCollectorMapping.properties file. You can copy and use the sample properties file provided by entering the following commands:

   ```
   cd %BINDIR%
   cd tcmremed\cfg
   copy WorkflowPostureCollectorMapping.properties.sample \
   WorkflowPostureCollectorMapping.properties
   ```


Downloaded from www.Manualslib.com manuals search engine

This file contains the mapping between the remediation workflows and the posture collector parameters used in the compliance policies defined on the Tivoli Security Compliance Manager server.

4. Edit the WorkflowPostureCollectorMapping.properties file and provide the content that will be relevant to the policies you have defined in the 6.2.4, “Customization of compliance policies” on page 161.

   For our compliance checks we have defined the following workflow names:

   – TCRNavScan
   – TCRNavVirusDefUpdate
   – TCRNavSoftwareInstalled
   – TCRMSPatchesInstallWinXP
   – TCRMSServicePackInstallWinXpSp2
   – TCRZLSoftwareInstalled
   – TCRZLSoftwareRunning
   – TCRMessengerDisabled

   The sample content of this file is presented in Example 8-1.

Example 8-1 WorkflowPostureCollectorMapping.properties contents

```
# <Workflow name>=<Posture collector class name>/<Parameter name>

TCRNavScan=nac.win.any.nav.PostureNavV2/SCAN_WF
TCRNavVirusDefUpdate=nac.win.any.nav.PostureNavV2/DEFS_WF
TCRNavSoftwareInstalled=nac.win.any.nav.PostureNavV2/VERSION_WF

TCRMSPatchesInstallWinXP=nac.win.any.hotfix.PostureHotfixV2/HOTFIX_WF

TCRMSServicePackInstallWinXpSp2=nac.win.any.oslevel.PostureOSLevelV2/SERVICE_PACK_WF

TCRZLSoftwareInstalled=nac.win.any.regkey.PostureRegKeyV2/KEY_WF

TCRZLSoftwareRunning=nac.win.any.services.PostureServices/SERVICE_RUNNING_WF

TCRMessengerDisabled=nac.win.any.services.PostureServices/SERVICE_DISABLED_WF

#TCRSolProcessRunning=nac.win.any.process.PostureProcess/PROCESS_RUNNING_WF
#TCRForbiddenFileExists=nac.win.any.file.PostureFile/FILE_EXISTS_WF

# --> Example workflow for Windows 2000 version of compliance policy
# TCRMSPatchesInstall=nac.win.any.hotfix.PostureHotfixV2/HOTFIX_WF
# TCRMSPatchesInstallW2K=nac.win.any.hotfix.PostureHotfixV2/HOTFIX_WF
# TCRMSServicePackInstallWin2kSp4=nac.win.any.oslevel.PostureOSLevelV2/SERVICE_PACK_WF
```

You must update this file for every collector type or workflow name you configured in your environment.

Downloaded from www.Manualslib.com manuals search engine

5. You must initialize the package creation utility environment. Issue the following commands:

   ```
   cd %BINDIR%
   cd tcmremed\cfg
   sputil_initial_setup.bat
   ```

   This creates the necessary objects on the Tivoli Configuration Manager, such as:

   – TcmRemedRegion Policy Region
   – TcmRemedProfMan Profile Manager
   – SPUtilConfig.properties file in the %BINDIR%\tcmremed\cfg directory

6. In the %BINDIR%\tcmremed\cfg directory there are several additional files. Some of them will be used as is, but some of them must be updated. For each pair of collector type and workflow type there is a separate configuration file containing the default remediation package options. These files are named using the following convention:

   ```
   <name_of_the_collector>_<workflow_type>.DefaultConfig.properties
   ```

   For example:

   ```
   nac.win.any.hotfix.PostureHotfixV2_HOTFIX_WF.DefaultConfig.properties
   ```

   By default there are nine files:

   – nac.win.any.nav.PostureNavV2_DEFS_WF.DefaultConfig.properties
   – nac.win.any.nav.PostureNavV2_SCAN_WF.DefaultConfig.properties
   – nac.win.any.nav.PostureNavV2_VERSION_WF.DefaultConfig.properties
   – nac.win.any.hotfix.PostureHotfixV2_HOTFIX_WF.DefaultConfig.properties
   – nac.win.any.oslevel.PostureOSLevelV2_SERVICE_PACK_WF.DefaultConfig.properties
   – nac.win.any.regkey.PostureRegKeyV2_KEY_WF.DefaultConfig.properties
   – nac.win.any.regkey.PostureRegKeyV2_VALUE_WF.DefaultConfig.properties
   – nac.win.any.services.PostureServices_SERVICE_RUNNING_WF.DefaultConfig.properties

   Most of them can be used as is, but a few must be edited. There is also a file missing for SERVICE_DISABLED_WF, so we have to create one named nac.win.any.services.PostureServices_SERVICE_DISABLED_WF.DefaultConfig.properties.

Downloaded from www.Manualslib.com manuals search engine

In Example 8-2 and Example 8-3 we present the final content required for the files that must be changed or added.

Example 8-2 nac.win.any.services.PostureServices_SERVICE_RUNNING_WF.DefaultConfig.properties file content

```
# SPUtil default config file for
nac.win.any.services.PostureServices_SERVICE_RUNNING_WF

#PostureCollectorName=nac.win.any.services.PostureServices
#PostureCollectorParameterName=SERVICE_RUNNING_WF

PackageName.input=NULLABLE
PackageName.format=${WorkflowName}

#EnableLogging=true

TmfWebUIPublicName.input=NULL
TmfWebUIPublicName.format=/${WorkflowName}/${PostureCollectorName}/${PostureCollectorParameterName}/latest
```

Example 8-3 nac.win.any.services.PostureServices_SERVICE_DISABLED_WF.DefaultConfig.properties file content

```
# SPUtil default config file for
nac.win.any.services.PostureServices_SERVICE_DISABLED_WF

#PostureCollectorName=nac.win.any.services.PostureServices
#PostureCollectorParameterName=SERVICE_DISABLED_WF

PackageName.input=NULLABLE
PackageName.format=${WorkflowName}

#EnableLogging=true

TmfWebUIPublicName.input=NULL
TmfWebUIPublicName.format=/${WorkflowName}/${PostureCollectorName}/${PostureCollectorParameterName}/latest
```

8.3 Creating remediation instructions for the users

With the Network Admission Control solution in place, a security administrator deploying a new policy must be aware of the possible side effects (for example, that a large number of noncompliant workstations may experience restricted

Downloaded from www.Manualslib.com manuals search engine

access to corporate intranet resources). To avoid serious business disruptions, necessary means should be taken to minimize this effect, including:

- Setting up a grace period for non-critical noncompliance situations
- Using traditional methods for large-scale fixes or software deployment before including them as mandatory in the security policy

One of the mandatory elements of the solution is a remediation process. It can, and should, be automated. However, the explanation of the corporate security policy and the remediation instructions should also be implemented. In this section we build instructional HTML pages for end users, which are presented to the user if there are any policy violations. The intention of these instructions is to guide the user to remediate the situation.

As a part of the IBM Integrated Security Solution for Cisco Networks deployment guide, several example HTML pages are included in the acme3.zip file. The guide is located at:

http://www.ibm.com/support/docview.wss?uid=swg24007082

These sample HTML pages are designed for the sample policy delivered in the package. This policy uses six posture collectors available at the time we wrote this book.

In the next few sections we describe the main rules of the HTML authoring guide.

8.3.1 Locating HTML

The HTML pages must exist on the client along with the policy containing the com.ibm.scm.nac.posture.PolicyCollector collector. They must reside in the client\scripts\ directory under the Security Compliance Manager main directory, typically in the C:\Program Files\IBM\SCM\client\scripts location.

Downloaded from www.Manualslib.com manuals search engine

The checks defined by the particular compliance objects within the policy relate to the data gathered by one posture collector. This means that the individual violations are collector-related, and this determines the way the HTML pages are organized. Figure 8-33 shows the directory structure that is required for the pages to be displayed properly.

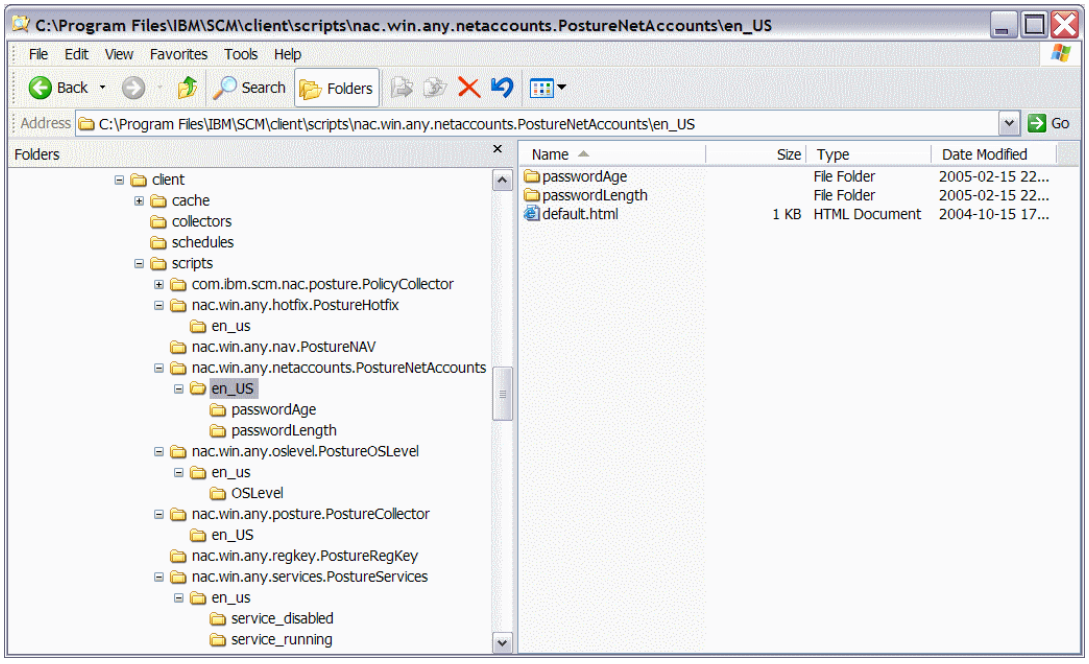


Figure 8-33 Directory structure for HTML pages

The first directory level below the scripts directory must be named after the collector (for example, nac.win.any.service.PostureServices). The next level below has to contain a separate directory for each language setting. For this book we use US English, so the subdirectory is named en_US.

The HTML displayed to the user is determined by searching the *scripts* tree starting with a best-case (most specific) match, and working upwards until a worst-case (default, no specific) match is found.

All pages must be named one of the following case-sensitive names:

- default.html
- PASS.html
- WARN.html
- FAIL.html
- ERROR.html

Additionally, all pages must be located in a subdirectory named from the ISO language/locale code the pages are written and encoded in. For example, Polish

Downloaded from www.Manualslib.com manuals search engine

pages would be in a subdirectory named *pl_PL*. The default language and local is *en_US*.

This document will use the variables listed in Table 8-1 to describe the dynamic parts of the paths to HTML pages.

Table 8-1 Variables definition

Variable	Definition
{DEFAULT_LANG}	Hard-coded to en_US.
{lang}	Preferred ISO language/locale code as detected by Java, for examples, pl_PL or en_AU.
{collector}	Name of the collector class that generated the element or item, for example, nac.win.any.netaccounts.PostureNetAccountsV2.
{instance}	Name of the instance that generated the element or item, for example, Windows Hotfixes.
{element}	Name of the posture element, for examples, KB665375 or Service Running.
{status}	Status of the posture element. Will be from the set: {PASS, WARN, FAIL, ERROR}.

Base HTML

The least specific set of HTML pages is the *base* HTML pages. These are the pages that are used to display the main welcoming page when the remediation handler user interface is refreshed or loaded, and the page displayed when no specific information is available for a selected item or element.

When the base HTML page is requested, the user interface will search in the following order:

```
scripts/nac.win.any.posture.PostureCollector/{lang}/default.html
scripts/nac.win.any.posture.PostureCollector/{DEFAULT_LANG}/default.html
```

If no match is found, a blank page will be displayed.

Posture item HTML

Each instance of posture collector generates exactly one *posture item*. The user interface searches for HTML in the following order of preference:

```
scripts/{collector}/{lang}/{instance}/default.html
scripts/{collector}/{lang}/default.html
scripts/{collector}/{DEFAULT_LANG}/{instance}/default.html
scripts/{collector}/{DEFAULT_LANG}/default.html
```


Downloaded from www.Manualslib.com manuals search engine

If none of these locations contain a valid page, the user interface falls back to the method used to locate the base HTML page.

HTML pages example

Assume that a policy wants to ensure that the ZoneAlarm and Remote Desktop services are running, and that several other services are not running. For clarity, the author might create three instances of the nac.win.any.services.PostureServicesV2 collector, and name one instance ZoneAlarm Firewall, one Remote Desktop Service, and one Forbidden Services. The policy wants to provide specific information about the ZoneAlarm and Remote Desktop services, but does not have anything special to say about the forbidden services.

Additionally, the policy only has some pages in Polish, and the rest are in English. The resulting document tree might look like this:

```
scripts/nac.win.any.services.PostureServicesV2/en_US/ZoneAlarm
Firewall/default.html
scripts/nac.win.any.services.PostureServicesV2/en_US/Remote Desktop
Service/default.html
scripts/nac.win.any.services.PostureServicesV2/pl_PL/ZoneAlarm
Firewall/default.html
scripts/nac.win.any.services.PostureServicesV2/pl_PL/default.html
scripts/nac.win.any.services.PostureServicesV2/en_US/default.html
```

For the pl_PL language/locale, pages that would be displayed for each item are presented in Table 8-2.

Table 8-2 Pages selected for pl_PL local

Posture item	**Displayed page relative to scripts/nac.win.any.services.PostureServicesV2/**
ZoneAlarm Firewall	pl_PL/ZoneAlarm Firewall/default.html
Remote Desktop Service	pl_PL/default.html
Forbidden Services	pl_PL/default.html

For the en_US language/locale, pages that would be displayed for each item are presented in Table 8-3.

Table 8-3 Pages selected for en_US local

Posture item	**Displayed page relative to scripts/nac.win.any.services.PostureServicesV2/**
ZoneAlarm Firewall	en_US/ZoneAlarm Firewall/default.html
Remote Desktop Service	en_US/Remote Desktop Service/default.html

Downloaded from www.Manualslib.com manuals search engine

Posture item	Displayed page relative to scripts/nac.win.any.services.PostureServicesV2/
Forbidden Services	en_US/default.html

Posture element HTML

Each *posture element* has a unique name and status. The user interface will first attempt to find pages that are specific to the item's name and status before moving to more general instance-level pages.

The user interface searches for HTML in the following order of preference:

```
scripts/{collector}/{lang}/{instance}/{element}/{status}.html
scripts/{collector}/{lang}/{instance}/{element}/default.html
scripts/{collector}/{lang}/{instance}/{status}.html
scripts/{collector}/{lang}/{instance}/default.html
scripts/{collector}/{lang}/{status}.html
scripts/{collector}/{lang}/default.html
scripts/{collector}/{DEFAULT_LANG}/{instance}/{element}/{status}.html
scripts/{collector}/{DEFAULT_LANG}/{instance}/{element}/default.html
scripts/{collector}/{DEFAULT_LANG}/{instance}/{status}.html
scripts/{collector}/{DEFAULT_LANG}/{instance}/default.html
scripts/{collector}/{DEFAULT_LANG}/{status}.html
scripts/{collector}/{DEFAULT_LANG}/default.html
```

If no pages age found at the instance level, the user interface will fall back to searching for the HTML of the element's parent posture Item.

8.3.2 Variables and variable tags

Variables are special tags that can be used to customize the information in the HTML pages presented to the user. Before a page is displayed the user interface parses it and attempts to substitute values for any variable tags found. If a variable tag is present in the HTML but does not have a value, the tag is removed.

There are three types of variable tags, each of which comes from a different aspect of the Security Compliance Manager solution. All of the tags have a similar syntax, which is shown below:

```
<wfattribute:name>
<field:name>
<remattribute:name>
```

The type of tag is followed by a colon (:) and an identifier. The entire tag is enclosed in the angle braces. A closing tag or slash (/) is not required or supported.

Downloaded from www.Manualslib.com manuals search engine

The wfattribute tag

The simplest variables are workflow attributes. When a posture collector performs a check that fails, it will often associate a *workflow* object with the element. The workflow object may contain one or more named lists of *attributes*. These attributes may be accessible using the wfattribute tag. When a workflow tag refers to a list with more than one item, the items are listed separated by commas. For example, a collector that checks for a required list of users might have the following attribute lists:

```
current_values
jdoe
ssmith
admin
required_values
jdoe
ssmith
admin
secureadmin
files
/etc/users
```

Table 8-4 shows possible HTML and the output that would result.

Table 8-4 Usage of wfattribute tag

HTML	Output
<html> <head> <head> <body> Current Values: <wfattribute:current_values> <p> Required Values: <wfattribute:required_values> <p> Files: <wfattribute:files> <p> Details: <wfattribute:details> </body> </html>	Current values: jdoe, ssmith, admin Required values: jdoe, ssmith, admin, secureadmin Files: /etc/users Details:

The field Tag

The field tag is used to access information contained in the actual *posture element* and *posture item* objects.

Downloaded from www.Manualslib.com manuals search engine

Table 8-5 presents the field names that may be used when a posture item is selected.

Table 8-5 The field tag usage on posture item level

Tag	Description	Example
<field:instancename>	Name of the selected instance.	Symantec Antivirus
<field:instanceid>	Identifier of the selected instance.	10
<field:collectorname>	Name of the generating collector.	nac.win.any.nav.PostureNavV2
<field:collectorid>	Identifier of the generating collector.	36
<field:collectiontime>	Time stamp collection was performed.	2005-11-10 08:32:06.0
<field:statuscounts>	Status of item's elements.	{PASS=1, FAIL=2}

Table 8-6 presents the field names that may be used when a posture element is selected.

Table 8-6 The field tag usage on posture element level

Tag	Description	Example
<field:name>	Name of the selected element	Virus definitions.
<field:status>	Status of the selected element	FAIL.
<field:msg>	Message associated with the selected element	Definitions are out of date.

The remattribute tag

The remattribute tag is used to access information to the remediation attributes present in the remediation user interface. These attributes come from various sources. Some attributes are generated by the Tivoli Security Compliance Manager client, and the others come from either the local handlers.properties file or from the HANDLERS_ATTRIBUTES parameter of the policy collector.

Downloaded from www.Manualslib.com manuals search engine

The attributes that are generated by the Security Compliance Manager client are always present, and are known as innate attributes. These attributes, presented in Table 8-7, cannot be overridden by user settings.

Table 8-7 Innate rematttribute tag usage

Attribute	Example	Description
client.alias	scmclient	The client's alias. This may be null if the client is not a DHCP client
client.dhcp	false	Indicates whether the client is a DHCP client.
client.fingerprint	a3:55:e5:62:2a:db:52:93:3b:c2:22:38:44:53:bf:02	The client's globally unique fingerprint.
client.id	1	The client's unique identifier as set by the server.
client.root	C:\PROGRA~1\IBM\SCM\client	The root of the client installation.
os.arch	x86	The processor architecture of the client as reported by Java.
os.name	Windows 2000	The host OS name as reported by Java.
os.version	5.0	The host OS version as reported by Java.
win.build	2195	The build version of Windows as reported in the CurrentBuildNumber registry key.
win.product	Microsoft Windows 2000	The name of the Windows product as reported in the ProductName registry key
win.sp	Service Pack 4	The Service Pack of the Windows product as reported in the CSDVersion registry key.
win.version	5.0	The version of Windows as reported in the CurrentVersion registry key.

All other attributes come from either the HANDLER_ATTRIBUTES parameter of the policy collector or the local handlers.properties file. In both of these locations attributes are specified in key-value pairs, separated by an equals sign (=). In general, attributes are used to control the configuration and behavior of the remediation subsystem, but they can also be used to provide general

Downloaded from www.Manualslib.com manuals search engine

information. For example, to enable the user interface to display the Fix Now button even if a remediation URL has not been sent, the following entry could be made in either the HANDLER_ATTRIBUTES or handlers.properties file:

```
remediationdialog.urlRequiredForRemediation=false
```

Because attributes can be set in multiple places, it is possible for them to conflict. To resolve these conflicts, the policy collector uses the following logic:

- Innate attributes cannot be overridden.
- Attributes set in HANDLER_ATTRIBUTES override those set in the handlers.properties file.

Examples are:

- Setting "client.id=1234" in either the HANDLER_ATTRIBUTES or handlers.properties has no effect.
- Setting "remediationdialog.logSearchPath=false" in HANDLER_ATTRIBUTES and "remediationdialog.logSearchPath=true" in handlers.properties results in the attribute being set to false.

Additionally, providing multiple entries with the same key name in the same location will result in one value being used only, and which value is arbitrary. For example, setting the following will result in extrajars being set to either logging.jar or uiprovider.jar, but which one is arbitrary.

```
extrajars=logging.jar
extrajars=uiprovider.jar
```

8.3.3 Debug attributes

Writing posture policy HTML can be a complex task. To simplify some aspects, a few debugging attributes are provided by the default remediation user interface. All of these attributes require that the "debug=true" setting is present in the "[debug]" section of the client.pref file.

Like all attributes, these attributes may be specified in either the handlers.properties file or the HANDLER_ATTRIBUTES parameter of the policy collector.

Logging available attributes

To enable logging of the attributes available for use with remattribute tags, the following attribute should be set:

```
remediationdialog.logAttributes=true
```


Downloaded from www.Manualslib.com manuals search engine

The attributes will be listed each time a posture element is selected (they are not logged when a posture item is selected). For example:

```
Attribute: os.arch -> x86
Attribute: client.dhcp -> false
Attribute: client.fingerprint ->
63:9A:42:AC:DE:13:41:59:F1:D2:11:96:7C:24:AF:90
Attribute: win.build -> 2600
Attribute: win.product -> Microsoft Windows XP
Attribute: os.name -> Windows XP
Attribute: os.version -> 5.1
Attribute: client.root -> C:\PROGRA~1\IBM\SCM\client
Attribute: win.sp -> Service Pack 2
Attribute: win.version -> 5.1
Attribute: client.id -> 2
Attribute: client.alias -> scmxp
```

Logging posture items

To enable logging of posture items and their posture elements, the following attribute should be set:

```
remediationdialog.logItems=true
```

When this attribute is set, the entire posture item tree will be logged each time an item is selected, including any associated posture elements, workflows, and workflow attributes. For example:

```
[20051110 08:34:45.545] PostureItem
                        |-instance : Symantec Antivirus (id: 12)
                        |-collector: nac.win.any.nav.PostureNavV2 (id: 3)
                        |-timestamp: 2005-11-10 08:23:06.0
                        |
                        |--PostureElement
                        |   |-name  : Version
                        |   |-status: PASS
                        |   `-msg   :
                        |
                        |--PostureElement
                        |   |-name  : Virus Definitions
                        |   |-status: FAIL
                        |   |-msg   : Definitions are out of date.
                        |   |
                        |   `--Workflow
                        |       |-id: DEFS_WF
                        |       |-parameters
                        |       `-attributes
                        |          `-attr: current_values
                        |             `-2005-10-26 00:00:00.0
                        |
```


Downloaded from www.Manualslib.com manuals search engine

```
`--PostureElement
    |-name  : Last Scan
    |-status: FAIL
    |-msg   : Scan is out of date.
    |
    `--Workflow
        |-id: SCAN_WF
        |-parameters
        `-attributes
           `-attr: current_values
              `-1003
```

Logging the HTML search path

To enable logging of the paths searched to locate HTML files, the following attribute should be set:

```
remediationdialog.logSearchPath=true
```

When this attribute is set, the paths searched are logged to the client.log file. For example:

```
File: scripts\nac.win.any.oslevel.PostureOSLevelV2\en_US\Windows Service
Pack\Windows Service Pack Level\PASS.html  ==> not found
File: scripts\nac.win.any.oslevel.PostureOSLevelV2\en_US\Windows Service
Pack\Windows Service Pack Level\default.html  ==> not found
File: scripts\nac.win.any.oslevel.PostureOSLevelV2\en_US\Windows Service
Pack\PASS.html  ==> found
```

This concludes the general HTML authoring principle section. In the next sections we describe the actual content created for the ABBC environment.

Downloaded from www.Manualslib.com manuals search engine

8.3.4 Creating HTML pages for ABBC policy

Figure 8-34 summarizes the directory structure for the HTML remediation pages used in our example.

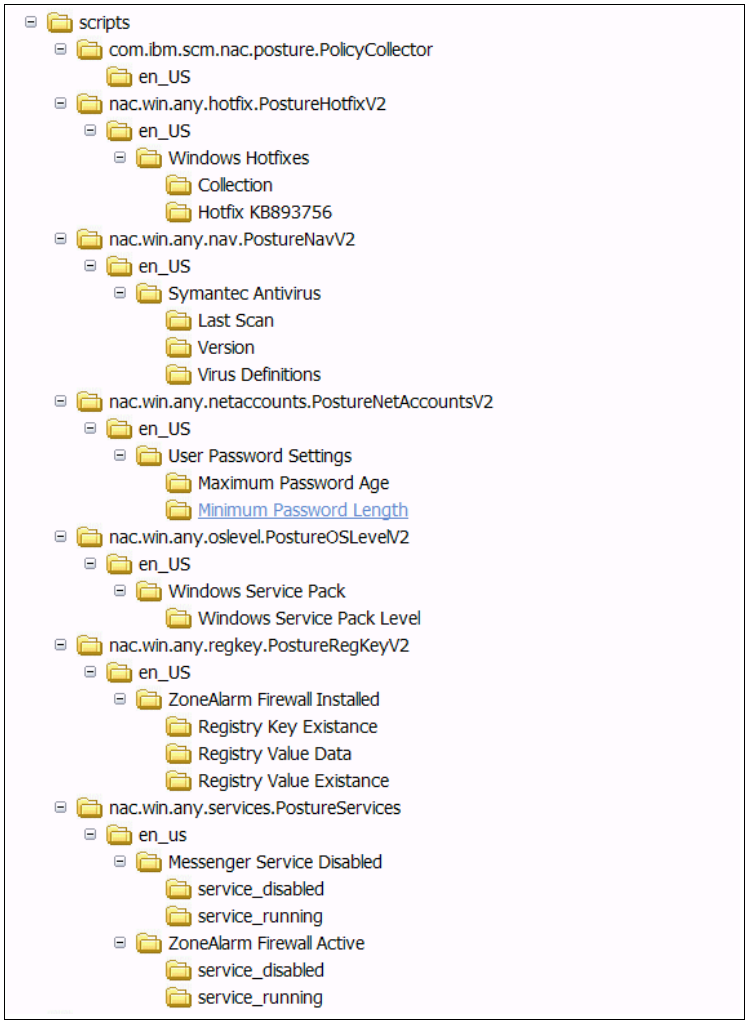


Figure 8-34 Sample directory structure for ABBC

The following three steps build meaningful HTML examples for the policies described in “Security compliance criteria” on page 100.

1. Our example policy specifies the following requirements: Local workstation password quality must meet the following criteria:

   – Password age must not be older than 90 days.
   – Password length must be at least eight characters.

   This policy is implemented using the posture collector nac.win.any.netaccounts.PostureNetAccountsV2.

Downloaded from www.Manualslib.com manuals search engine

First we create the default.html page describing these basic requirements and save it in the nac.win.any.netaccounts.PostureNetAccountsV2\en_US\ directory, as shown in Figure 8-34 on page 409. Figure 8-35 shows the sample page layout as presented to the user in the remediation user interface.

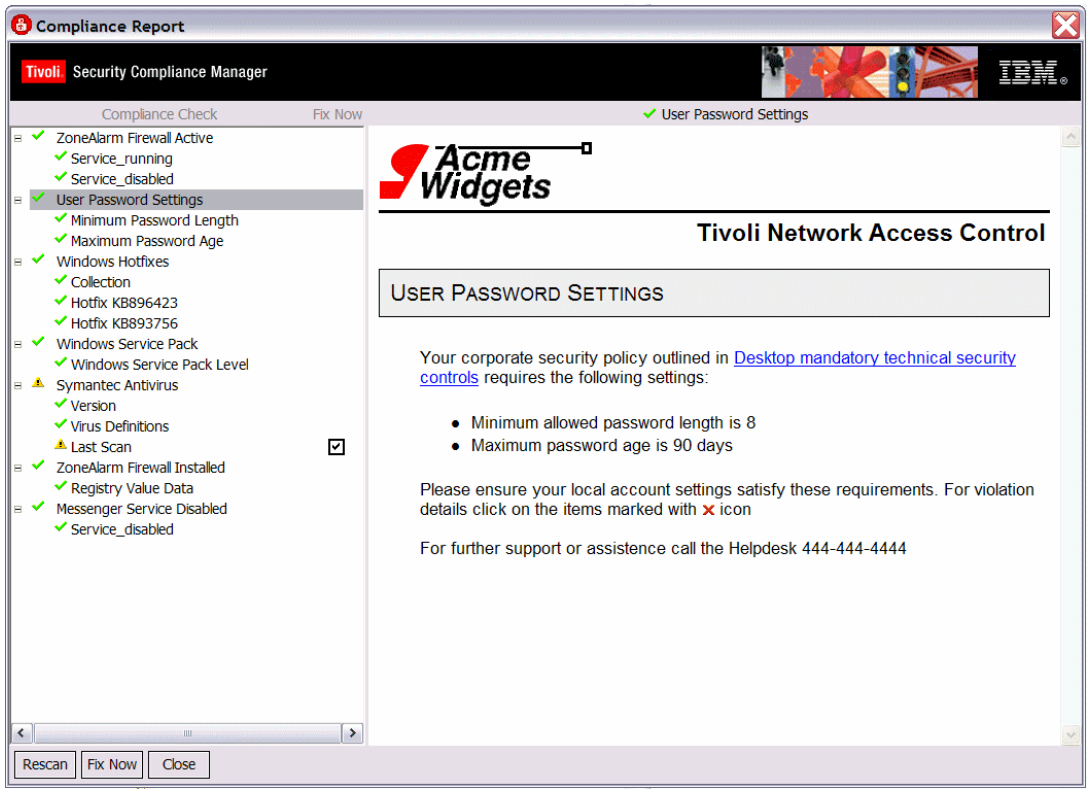


Figure 8-35 Sample ABBC Corp. security policy description page

Example 8-4 shows the HTML source code for this page.

Example 8-4 HTML source for password policy settings page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">
<script type="text/javascript"></script>
<style type="text/css" media="all">
   @import
"file:/c:/Progra~1/IBM/SCM/client/scripts/com.ibm.scm.nac.posture.PolicyCol
lector/sentry.css";
</style>
<title>

</title>
</head>
<body>
```


Downloaded from www.Manualslib.com manuals search engine

```
<div id="Logo"></div>
<div id="MajorTitle">
Tivoli Network Access Control
</div>
<br>
<div id="SectionTitle">

<!-- BEGIN SECTION HEADING TEXT -->
<field:instancename> <field:name>
<!-- END SECTION HEADING TEXT -->

</div>
<div id="DetailText">
Your corporate security policy outlined in
<a href="http://w3.abbc.com/security/desktop">Desktop mandatory technical
security controls</a> requires the following settings:<br>
<ul>
  <li>Minimum allowed password length is 8</li>
  <li>Maximum password age is 90 days<br>
  </li>
</ul>
Please ensure your local account settings satisfy these requirements.
For violation details click the items marked with <image
src="file:/c:/Program
Files/IBM/SCM/client/scripts/com.ibm.scm.nac.posture.PolicyCollector/images
/icon-fail.gif"> icon
<br><br>
For further support or assistence call the Helpdesk 444-444-4444
<br>
<!-- END ITEM DETAIL TEXT -->
</div></body>
</html>
```

This page uses a style defined in the separate sentry.css file, which was copied to the directory c:\Program Files\IBM\SCM\client\scripts\com.ibm.scm.nac.posture.PolicyCollector along with any custom graphic files used on all the HTML pages, such as the company's logo. Example 8-5 shows the content of the CSS file.

Example 8-5 Content of style definition file

```
#Logo {
   padding: 0px;
   margin: 0px;
   border-style:solid;
   border-color:black;
   border-width:0px 0px 3px 0px;
   line-height:3px;
```


Downloaded from www.Manualslib.com manuals search engine

```
   background: #fff
url("file:///C:/Progra~1/IBM/SCM/client/scripts/com.ibm.scm.nac.posture.Pol
icyCollector/logo.gif") no-repeat top left;
   height: 70px;
   }

#SectionTitle {
   margin:10px 0px 10px 0px;
   padding:10px 10px 10px 10px;
   border-style:solid;
   border-color:black;
   border-width:1px 1px;
   background-color:#eee;
   font: 13pt arial;
   font-weight: 500;
   font-variant: small-caps;
}

#MajorTitle {
  padding:5px 4px 0px 0px;
  font: 14 pt arial;
  font-weight: 700;
  text-align: right;
}

#DetailText {
  padding: 20px 0px 0px 40px;
  font-family: sans-serif;
  font-size: 10pt;
}
```

2. The default.html page resembles a generic description of the policy, so we prepare additional pages describing particular checks in more detail, along with instructions for the user to regain compliance. The collector we use as an example supports two checks:
   - Minimum password length
   - Maximum password age

Downloaded from www.Manualslib.com manuals search engine

To prepare separate descriptions for each of these conditions we create two subdirectories named after the checks. In the Minimum Password Length subdirectory we create an HTML page named WARN.html, shown in Figure 8-36.

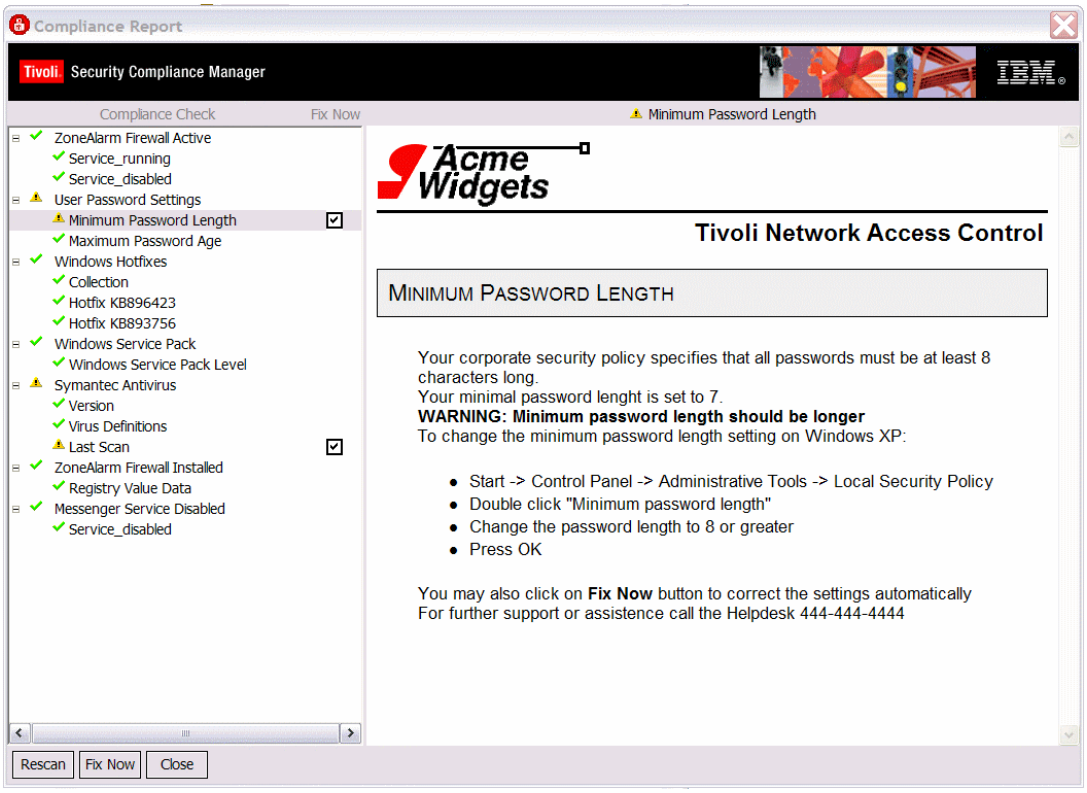


Figure 8-36 Minimum password length HTML warning page

This page includes simple instructions to the user for changing the minimum password length setting. This page mostly consists of static HTML, shown in Example 8-6. It also introduces some of the tags described in 8.3.2, “Variables and variable tags” on page 402.

Example 8-6 HTML source for password length policy details page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">
<script type="text/javascript"></script>
<style type="text/css" media="all">
   @import "file:/c:/Program
Files/IBM/SCM/client/scripts/com.ibm.scm.nac.posture.PolicyCollector/sentry
.css";
</style>
<title>
```


Downloaded from www.Manualslib.com manuals search engine

```
</title>
</head>
<body>
<div id="Logo"></div>
<div id="MajorTitle">
Tivoli Network Access Control
</div>
<br>
<div id="SectionTitle">
<!-- BEGIN SECTION HEADING TEXT -->
<field:instancename> <field:name>
<!-- END SECTION HEADING TEXT -->
</div>
<div id="DetailText">
<!-- BEGIN ITEM DETAIL TEXT -->
Your corporate security policy specifies that all passwords must be at
least 8 characters long.<br>
Your minimal password lenght is set to
<wfattribute:current_values>.<br><b>WARNING: <field:msg></b><br>
To change the minimum password length setting on Windows XP:<br><br>
<ul>
  <li>Start -&gt; Control Panel -&gt; Administrative Tools -&gt; Local
Security Policy<br>
  </li>
  <li>Double click "Minimum password length"</li>
  <li>Change the password length to 8 or greater</li>
  <li>Press OK<br>
  </li>
</ul>
You may also click <b>Fix Now</b> button to  correct the settings
automatically<br>
For further support or assistence call the Helpdesk 444-444-4444<br>
<!-- END ITEM DETAIL TEXT -->
</div>
</body>
</html>
```


Downloaded from www.Manualslib.com manuals search engine

3. Understanding the tags described in the previous step, we now build a more sophisticated HTML page for maximum password age check named FAIL.html. This page will be used when the compliance check generates the FAIL status. Figure 8-37 shows the resulting page.

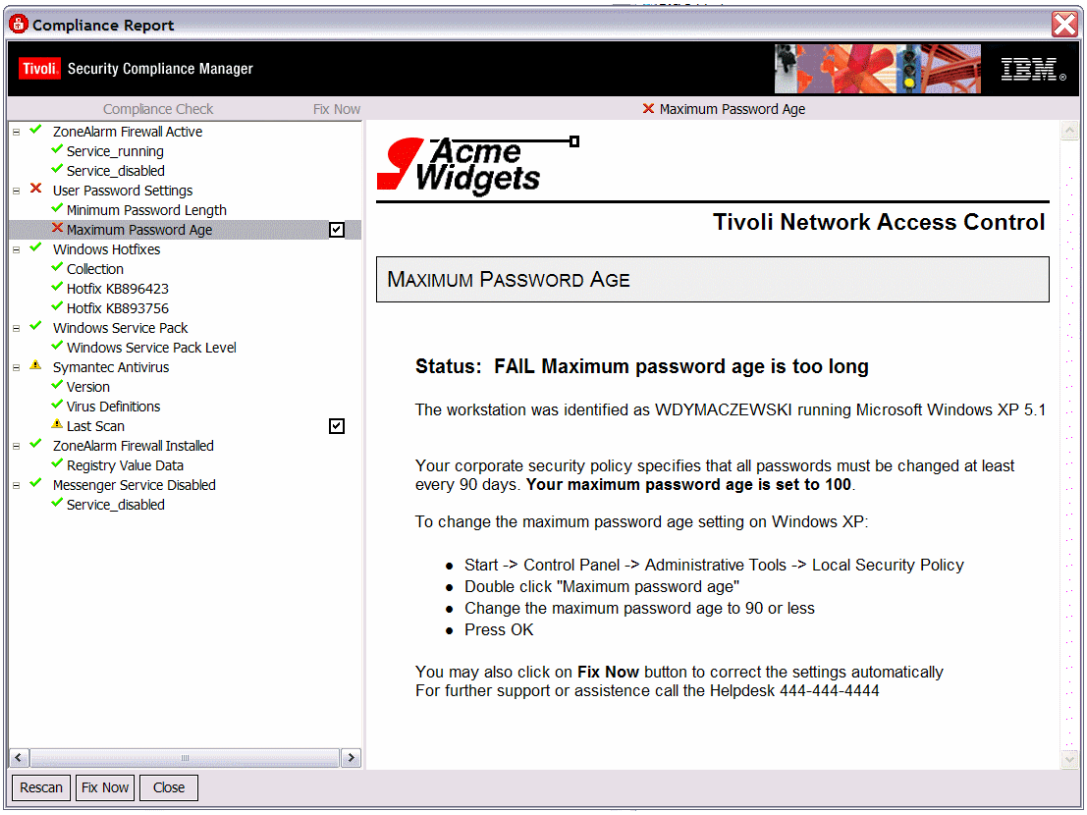

Compliance Report
Tivoli Security Compliance Manager
IBM
Compliance Check
Fix Now
Maximum Password Age
ZoneAlarm Firewall Active
Service_running
Service_disabled
User Password Settings
Minimum Password Length
Maximum Password Age
Windows Hotfixes
Collection
Hotfix KB896423
Hotfix KB893756
Windows Service Pack
Windows Service Pack Level
Symantec Antivirus
Version
Virus Definitions
Last Scan
ZoneAlarm Firewall Installed
Registry Value Data
Messenger Service Disabled
Service_disabled
Acme Widgets
Tivoli Network Access Control
MAXIMUM PASSWORD AGE
Status: FAIL Maximum password age is too long
The workstation was identified as WDYMACZEWSKI running Microsoft Windows XP 5.1
Your corporate security policy specifies that all passwords must be changed at least every 90 days. Your maximum password age is set to 100.
To change the maximum password age setting on Windows XP:
Start -> Control Panel -> Administrative Tools -> Local Security Policy
Double click "Maximum password age"
Change the maximum password age to 90 or less
Press OK
You may also click on Fix Now button to correct the settings automatically
For further support or assistence call the Helpdesk 444-444-4444
Rescan
Fix Now
Close

Figure 8-37 Maximum password age HTML page

Example 8-7 shows the HTML source for the page.

Example 8-7 HTML source for password age policy details page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">
<script type="text/javascript"></script>
<style type="text/css" media="all">
   @import "file:/c:/Program
Files/IBM/SCM/client/scripts/com.ibm.scm.nac.posture.PolicyCollector/sentry
.css";
</style>
<title>
</title>
</head>
<body>
```


Downloaded from www.Manualslib.com manuals search engine

```
<div id="Logo"></div>
<div id="MajorTitle">
Tivoli Network Access Control
</div>
<br>
<div id="SectionTitle">
<!-- BEGIN SECTION HEADING TEXT -->
<field:instancename> <field:name>
<!-- END SECTION HEADING TEXT -->
</div>
<div id="DetailText">
<!-- BEGIN ITEM DETAIL TEXT -->
<h4>Status:  <field:status> <field:msg></h4>
The workstation was identified as <rematttribute:client.alias> running
<rematttribute:win.product> <rematttribute:win.version>
<br><br>
Your corporate security policy specifies that all passwords must be changed
at least every 90 days.
<b>Your maximum password age is set to
<wfattribute:current_values></b>.<br>
<br>
To change the maximum password age setting on Windows XP:<br>
<br>
<ul>
  <li>Start -&gt; Control Panel -&gt; Administrative Tools -&gt; Local
Security Policy<br>
  </li>
  <li>Double click "Maximum password age"</li>
  <li>Change the maximum password age to 90 or less</li>
  <li>Press OK<br>
  </li>
</ul>
You may also click <b>Fix Now</b> button to  correct the settings
automatically<br>
For further support or assistence call the Helpdesk 444-444-4444
<br>
<!-- END ITEM DETAIL TEXT -->
</div>
</body>
</html>
```

As you may have noticed, some of the runtime data is presented to the user. These tags may also be used to build the client-related URL. This may be used to prepare detailed OS version-dependent user instructions on a separate Web server, and to provide the user with a direct link to the patch file required for particular operating system levels.

Downloaded from www.Manualslib.com manuals search engine

You can build similar pages for all of the compliance checks described in your policy. In the next section we provide the detailed steps to build the remediation workflows called when the user clicks the Fix Now button on the remediation user interface.

8.4 Building the remediation workflows

The complexity of creating the actual remediation packages can vary greatly depending on what you are trying to achieve and your Tivoli Configuration Manager skills.

The remediation packages are called *remediation workflows* because of the Tivoli Provisioning Manager heritage. In the current version of the solution they resemble the normal software package block files published on the Tivoli Configuration Manager Web Gateway server and installed locally on the noncompliant workstation using the standalone Tivoli Configuration Manager commands. However, in this book we use the terms *remediation workflow* and *remediation package* interchangeably.

Software package block (SPB) is a native format of the Tivoli software distribution products, used with Tivoli Configuration Manager as well as with the latest version of Tivoli Provisioning Manager and Tivoli Provisioning Manager for Software.

You can create and edit SPB packages using several different tools, like:

- The Java-based *Software Package Editor* included with Tivoli Configuration Manager
- Command-line tools
- The Eclipse-based Software Package Editor included with Tivoli Provisioning Manager for Software

In addition to the choices listed above you can use the sputil.sh utility provided with the *IISSCN extension pack2 for Tivoli Configuration Manager*, which is a wrapper for Tivoli Configuration Manager commands.

As this book is not meant to be a comprehensive Tivoli Configuration Manager manual, in the next paragraphs we describe how to use this utility to build the remediation packages required for the policies we have defined in 6.2.4, “Customization of compliance policies” on page 161.

Downloaded from www.Manualslib.com manuals search engine

While editing our policy in 6.2, “Configuration of the compliance policies” on page 152, we have defined the following workflow names to be used for automated remediation:

- TCRNavScan
- TCRNavVirusDefUpdate
- TCRNavSoftwareInstalled
- TCRMSPatchesInstallWinXP
- TCRMSServicePackInstallWinXpSp2
- TCRZLSoftwareInstalled
- TCRZLSoftwareRunning
- TCRMessengerDisabled

For each of them there must be a remediation package defined and published on the Tivoli Configuration Manager Web Gateway server.

Below we describe how to build all of the packages, one by one.

TCRNavScan workflow

The *TCRNavScan* workflow was defined in the SCAN_WF parameter in the Symantec Antivirus policy to be used when the compliance check generated a FAIL or WARNING status. The purpose of the workflow is to initiate the Symantec Antivirus scan. In this case, for simplicity’s sake, the workflow will only instruct the user on how to initiate the scan using the graphical user interface.

Assuming the above, the software package block we must build is very simple. It will contain a Visual Basic® script that pops up a window with the instructions for the user.

The steps to create and publish the TCRNavScan remediation package using the sputil.sh utility are:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRNavScan
cd TCRNavScan
```


Downloaded from www.Manualslib.com manuals search engine

2. In the next step we create the Windows script that will perform the actual job. We can reuse the one provided with the samples in the sample_TCRNavScan directory named NavScanMessage_en.wsf (Windows Script File format) or create a new one using the source code provided in Example 8-8. Copy the file to the new directory that you created in the previous step.

Example 8-8 Content of NavScanMessage_en.wsf

```
<?xml version="1.0"?>
<job>
  <script language="JScript">
    <![CDATA[
      var WshShell = WScript.CreateObject("WScript.Shell");
      var strTitle = "Tivoli Security Compliance Manager";
      var nSecondsToWait = 0;
      var nButtonType_Ok = 0;
      var nIconType_Exclamation = 48;
      var nType = nButtonType_Ok + nIconType_Exclamation;
      WshShell.Popup("A virus scan of your system must be performed. Please
follow the steps below. \n\nPlease open Symantec/Norton AntiVirus GUI from
Start -> Programs -> Symantec Client Security -> Symantec AntiVirus. Then
click Scan -> Scan Computer. Indicate that all local drives are to be
scanned, and then click Scan to begin the scan.", nSecondsToWait, strTitle,
nType);
    ]]>
  </script>
</job>
```


Downloaded from www.Manualslib.com manuals search engine

3. Next we create the configuration file for the sputil.sh utility containing the instructions how to build the package. Copy the Sample.properties file from sample_TCRNavScan directory to the TCRNavScan directory and edit it with the text editor to match the content specified in Example 8-9. Especially make sure that:

   WorkflowName Equals the name of the workflow that matches the value of the SCAN_WF parameter in the policy.

   SourceFilename[0] Equals the name for the script file located in the same directory.

   TmfWebUIEndpoint Equals the name of the Tivoli Framework endpoint located on the Web Gateway. If you followed the installation instruction from this book it will be the host name of that server.

   Leave the other values as is. They are used by the utility during the package creation.

   Example 8-9 Content of Sample.properties file for TCRNavScan

```
#The WorkflowName parameter below will determine the name of the package
#Make sure it matches the name of the one you want to generate
WorkflowName=TCRNavScan

SourceFilename.arrayLength=1
DestinationPath.arrayLength=1

SourceFilename[0]=NavScanMessage_en.wsf

RegistryKeyForExePathName.arrayLength=1
ExeName.arrayLength=1
ExeArg.arrayLength=1

RegistryKeyForExePathName[0]=
ExeName[0].format=wscript.exe
ExeArg[0].arrayLength=1
ExeArg[0][0].format="${DestinationPath[0]}"

# Specify the name of your endpoint in the line below
TmfWebUIEndpoint=tcmweb
```

4. Make sure that the Tivoli Object Dispatcher service is running. You may check it in the services window or by using the following command:

```
odadmin odlist
```


Downloaded from www.Manualslib.com manuals search engine

As a result you should see the output presented below:

```
Region           Disp  Flags  Port            IPaddr   Hostname(s)
1406765930          1    ct-    94   192.168.230.140   tcmweb
```

5. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

   ```
   cd $BINDIR/tcmremed/download
   cd TCRNavScan
   $BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
   ```

   As a result there are five files created. The three listed below are located in the $BINDIR/tcmremed/download/TCRNavScan directory:

   – TCRNavScan_sp.sh

     Shell script that creates the Software Package profile in a Tivoli Framework environment and imports the software package definition to create the final software package block.

   – TCRNavScan_publish.sh

     Shell script that publishes the Software Package profile to the Tivoli Configuration Manager Web Gateway.

   – TCRNavScanConfig.properties

     Final properties file as a result of combining the Sample.properties file specified as a parameter to the **sputil.sh** command and the default properties for this type of collector specified in nac.win.any.nav.PostureNavV2_SCAN_WF.DefaultConfig.properties and also in SPUtilConfig.properties. These two additional files are located in the $BINDIR/tcmremed/cfg directory and were briefly described in 8.2.4, “Installation of the Software Package Utilities” on page 394.

   You do not need to run any of these script files, as the sputil.sh utility does it for you. You may verify the result of running the tool with the following command:

   ```
   wlookup -ar SoftwarePackage | grep TCRNavScan
   ```

   If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment, as it is meant to be unique and it is associated with the Tivoli Management Region number):

   ```
   TCRNavScan^1.0  1406765930.1.846#SoftwarePackage::Spo#
   ```


Downloaded from www.Manualslib.com manuals search engine

Two additional files are created in the $BINDIR/tcmremed/work directory. These are:

TCRNavScan.spd Software package definition file. This is a text meta file containing all of the package configuration information.

TCRNavScan.spb Resulting software package block binary file. This file is being published on the Web page and is downloaded to the client workstation during the remediation process.

Important: These .spd and .spb files were created as a side effect of running the sputil.sh utility. Editing these files will not change the content of the package posted on the Web Gateway and used during remediation.

6. Now you are ready to test the remediation process. On a client workstation, which indicates to have the latest antivirus scan violation or warning, as shown on Figure 8-38, click the **Fix Now** button.

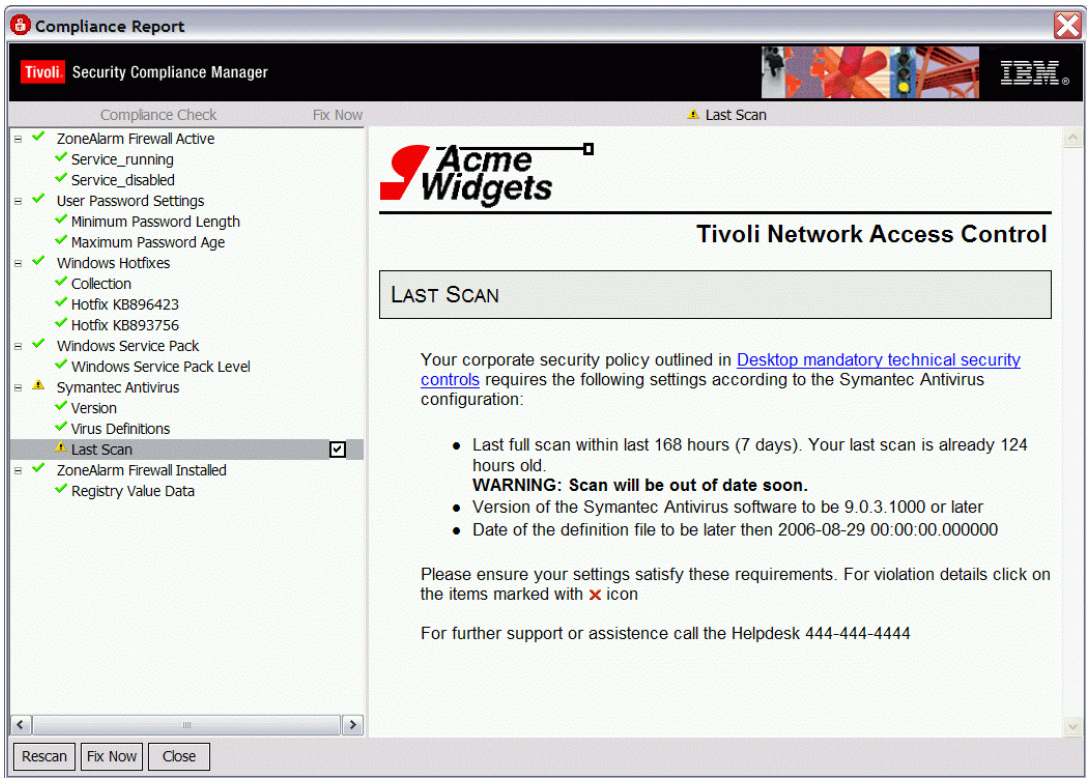

Compliance Report
Tivoli Security Compliance Manager
IBM
Compliance Check
Fix Now
Last Scan
ZoneAlarm Firewall Active
Service_running
Service_disabled
User Password Settings
Minimum Password Length
Maximum Password Age
Windows Hotfixes
Collection
Hotfix KB896423
Hotfix KB893756
Windows Service Pack
Windows Service Pack Level
Symantec Antivirus
Version
Virus Definitions
Last Scan
ZoneAlarm Firewall Installed
Registry Value Data
Acme Widgets
Tivoli Network Access Control
LAST SCAN
Your corporate security policy outlined in Desktop mandatory technical security controls requires the following settings according to the Symantec Antivirus configuration:
Last full scan within last 168 hours (7 days). Your last scan is already 124 hours old.
WARNING: Scan will be out of date soon.
Version of the Symantec Antivirus software to be 9.0.3.1000 or later
Date of the definition file to be later then 2006-08-29 00:00:00.000000
Please ensure your settings satisfy these requirements. For violation details click on the items marked with x icon
For further support or assistence call the Helpdesk 444-444-4444
Rescan
Fix Now
Close

Figure 8-38 Remediation handler interface with the warning

Downloaded from www.Manualslib.com manuals search engine

The remediation process window is displayed and the proper software package block is downloaded and executed. You are presented with the instructions shown in Figure 8-39.

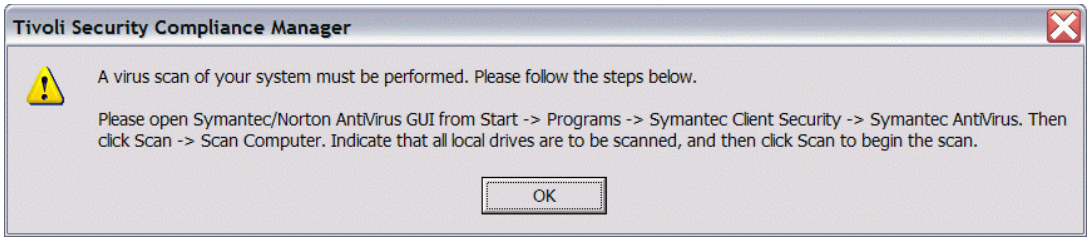

Tivoli Security Compliance Manager
A virus scan of your system must be performed. Please follow the steps below.
Please open Symantec/Norton AntiVirus GUI from Start -> Programs -> Symantec Client Security -> Symantec AntiVirus. Then click Scan -> Scan Computer. Indicate that all local drives are to be scanned, and then click Scan to begin the scan.
OK

Figure 8-39 Result of running NavScanMessage_en.wsf

When you click **OK** the final remediation handler window should look Figure 8-40.

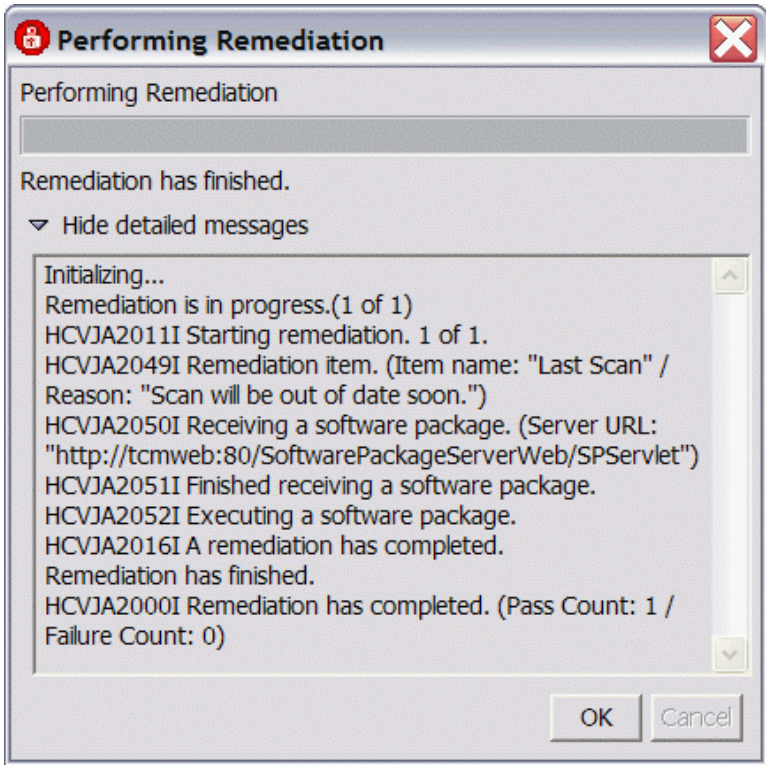

Performing Remediation
Performing Remediation
Remediation has finished.
Hide detailed messages
Initializing...
Remediation is in progress.(1 of 1)
HCVJA2011I Starting remediation. 1 of 1.
HCVJA2049I Remediation item. (Item name: "Last Scan" / Reason: "Scan will be out of date soon.")
HCVJA2050I Receiving a software package. (Server URL: "http://tcmweb:80/SoftwarePackageServerWeb/SPServlet")
HCVJA2051I Finished receiving a software package.
HCVJA2052I Executing a software package.
HCVJA2016I A remediation has completed.
Remediation has finished.
HCVJA2000I Remediation has completed. (Pass Count: 1 / Failure Count: 0)
OK
Cancel

Figure 8-40 Remediation handler status window

TCRNavVirusDefUpdate

The *TCRNavVirusDefUpdate* workflow was defined in the DEFS_WF parameter in the Symantec Antivirus policy to be used when the compliance check generated a FAIL or WARNING status. The purpose of the workflow is to initiate the Symantec Antivirus LiveUpdate process to download the new virus definition

Downloaded from www.Manualslib.com manuals search engine

file. The live update process is initiated with the vpdn_lu.exe executable located in the Symantec Antivirus home directory. When run with a /s flag the process runs silently in the background. Based on this knowledge we have to create the software package that executes this file. Follow the steps described below:

1. First open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRNavVirusDefUpdate
cd TCRNavVirusDefUpdate
```

2. Then create a configuration file for sputil.sh utility containing the instructions about how to build the package. Copy the Sample.properties file from the sample_TCRNavDefUpdate directory to the TCRNavDefUpdate directory and edit it with a text editor to match the content specified in Example 8-10.

Example 8-10 Sample.properties file for TCRNavVirusDefUpdate workflow

```
WorkflowName=TCRNavVirusDefUpdate

RegistryKeyForExePathName.arrayLength=2
ExeName.arrayLength=2
ExeArg.arrayLength=2

RegistryKeyForExePathName[0]=HKEY_LOCAL_MACHINE\\Software\\Symantec\\Instal
ledApps\\SAV Install Directory
ExeName[0]=vpdn_lu.exe
ExeArg[0].arrayLength=1
ExeArg[0][0]=/s

RegistryKeyForExePathName[1]=HKEY_LOCAL_MACHINE\\Software\\Symantec\\Instal
ledApps\\SAV Install Directory
ExeName[1]=vpdn_lu.exe
ExeArg[1].arrayLength=1
ExeArg[1][0]=/s

#RebootNowFlag=false
#RebootLaterFlag=false
#RebootRetryNumber=1

TmfWebUIEndpoint=tcmweb
```


Downloaded from www.Manualslib.com manuals search engine

3. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

```
cd $BINDIR/tcmremed/download
cd TCRNavVirusDefUpdate
$BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
```

4. Verify the result of running the tool with the following command:

```
wlookup -ar SoftwarePackage | grep TCRNavVirusDefUpdate
```

   If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with the Tivoli Management Region number):

```
TCRNavVirusDefUpdate^1.0        1406765930.1.847#SoftwarePackage::Spo#
```

TCRNavSoftwareInstalled

The *TCRNavSoftwareInstalled* workflow was defined in the VERSION_WF parameter in the Symantec Antivirus policy to be used when the compliance check generated a FAIL or WARNING status. The purpose of the workflow is to install the required version of the Symantec Antivirus software. To build this remediation package you must have the appropriate client license for Symantec Antivirus software and an installation file. Follow the steps described below:

1. First open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRNavSoftwareInstalled
cd TCRNavSoftwareInstalled
```

2. Copy to this directory with the Symantec Antivirus installation file. In our lab we used the file named SAV9_MR3_EN_WK.exe.

> **Attention:** Symantec Antivirus is a licensed software. You must obtain a proper license before using this software.

Downloaded from www.Manualslib.com manuals search engine

3. Create the configuration file for sputil.sh utility containing the instructions on how to build the package. Copy the Sample.properties file from the sample_TCRNavSoftwareInstalled directory to the TCRNavSoftwareInstalled directory and edit it with the text editor to match the content specified in Example 8-10 on page 424.

Example 8-11 Sample.properties file for TCRNavSoftwareInstalled workflow

```
WorkflowName=TCRNavSoftwareInstalled

SourceFilename.arrayLength=1
ExeArg.arrayLength=2

SourceFilename[0]=SAV9_MR3_EN_WK.exe
ExeArg[0].arrayLength=0
ExeArg[1].arrayLength=0

#RebootNowFlag=true
#RebootLaterFlag=false
#RebootRetryNumber=1

TmfWebUIEndpoint=tcmweb
```

4. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

```
cd $BINDIR/tcmremed/download
cd TCRNavSoftwareInstalled
$BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
```

5. Verify the result of running the tool with the following command:

```
wlookup -ar SoftwarePackage | grep TCRNavSoftwareInstalled
```

If the package was created, the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number):

```
TCRNavSoftwareInstalled^1.0        1406765930.1.848#SoftwarePackage::Spo#
```

This workflow is not perfect because it still pops up the installer window and asks the user for the temporary directory to unpack the files, but it is meant to be just the example.

TCRMSPatchesInstallWinXP

The *TCRMSPatchesInstallWinXP* workflow was defined in the HOTFIX_WF parameter in the Windows Hotfixes policy to be used when the compliance check generated a FAIL or WARNING status. The purpose of the workflow is to install

Downloaded from www.Manualslib.com manuals search engine

the missing hotfixes. As this policy checks for multiple hotfixes in parallel, the missing ones must be passed back to the remediation workflow as a parameter.

You must build the remediation package separately for each hotfix you have specified in the policy. As an example we used hotfix KB896423. Follow the steps described below, modifying the hotfix name according to the name you are using:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRMSPatchesInstallWinXP_KB896423
cd TCRMSPatchesInstallWinXP_KB896423
```

2. To build the package you must download the appropriate hotfix from the Microsoft Web site. KB896423 can be found at the following location:

   http://www.microsoft.com/downloads/details.aspx?familyid=EF4O2946-1C3B-47E9-9D51-77D89ODF8725&displaylang=en

   The file is named WindowsXP-KB896423-x86-ENU.exe. Copy it to the newly created directory TCRMSPatchesInstallWinXP_KB896423.

3. Create the configuration file for the sputil.sh utility containing the instructions on how to build the package. Copy the Sample.properties file from the sample_TCRMSPatchesInstall_KB896423 directory to the TCRMSPatchesInstallWinXP_KB896423 directory and edit it with the text editor to match the content specified in Example 8-12.

Example 8-12 Sample.properties file for TCRMSPatchesInstall_KB896423 workflow

```
WorkflowName=TCRMSPatchesInstallWinXP

SourceFilename.arrayLength=1
ExeArg.arrayLength=1

SourceFilename[O]=WindowsXP-KB896423-x86-ENU.exe
ExeArg[O].arrayLength=2
ExeArg[O][O]=/passive
ExeArg[O][1]=/norestart

#RunQchainFlag=true

#RebootNowFlag=false
#RebootLaterFlag=false
#RebootRetryNumber=1
```


Downloaded from www.Manualslib.com manuals search engine

```
HotfixId=KB896423
TmfWebUIEndpoint=tcmweb
```

4. This configuration file is a little different from the others created before. The first difference is the additional parameter close to the end named *HotfixId*. The value of this parameter *must* match the name of the hotfix. To notice the second difference, take a closer look into the nac.win.any.hotfix.PostureHotfixV2_HOTFIX_WF.DefaultConfig.properties file located in the $BINDIR/tcmremed/cfg directory. This file contains the default options for this type of the workflow. Specifically, there are three important parameters:

   ```
   RunQchainFlag.format=true
   TmfWebUIPublicName.format=/${WorkflowName}/${PostureCollectorName}/${Postur
   eCollectorParameterName}/${HotfixId}
   ```

   RunQchainFlag equaling true means that the software package block installer should use the qchain.exe utility, which is provided by Microsoft in order to provide the ability to install multiple hotfixes with only one reboot at the end of the installation. This line has two implications:

   – During the remediation you can install multiple hotfixes, one by another, without a reboot.

   – You must add this qchain.exe utility to your remediation package.

   This utility is a part of the Microsoft Windows 2000 Resource Kit and is available free for registered Microsoft Windows users. Download it from the Microsoft Web site and store it in the $BINDIR/tcmremed/cfg directory.

   Note: If you do not have or do not want to use the qchain.exe utility, set the value of the RunQchainFlag to false in the Sample.properties file for the hotfix remediation package you are preparing.

   The second parameter, TmfWebUIPublicName.format, defines the public name of the remediation package under which it will be seen on the Web Gateway. You may notice that the actual workflow name for all hotfix packages will be the same (TCRMSPatchesInstallWinXP), but the name of the package will include the HotfixId specified in the Sample.properties file.

5. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

   ```
   cd $BINDIR/tcmremed/download
   cd TCRMSPatchesInstallWinXP_KB896423
   $BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
   ```

6. Verify the result of running the tool with the following command:

   ```
   wlookup -ar SoftwarePackage | grep TCRMSPatchesInstallWinXP_KB896423
   ```


Downloaded from www.Manualslib.com manuals search engine

If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number):

```
TCRMSPatchesInstallWinXP_KB896423^1.0
1406765930.1.849#SoftwarePackage::Spo#
```

7. When a noncompliant client missing the KB896423 hotfix is remediated with the Fix Now button, a remediation handler window is shown, as depicted in Figure 8-41.

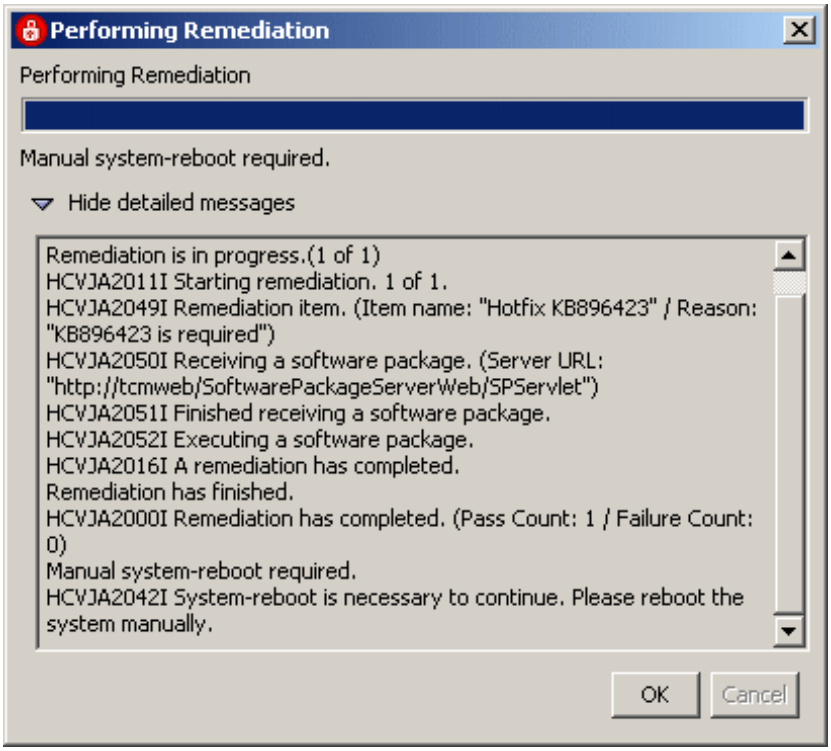

Performing Remediation
Performing Remediation
Manual system-reboot required.
Hide detailed messages
Remediation is in progress.(1 of 1)
HCVJA2011I Starting remediation. 1 of 1.
HCVJA2049I Remediation item. (Item name: "Hotfix KB896423" / Reason: "KB896423 is required")
HCVJA2050I Receiving a software package. (Server URL: "http://tcmweb/SoftwarePackageServerWeb/SPServlet")
HCVJA2051I Finished receiving a software package.
HCVJA2052I Executing a software package.
HCVJA2016I A remediation has completed.
Remediation has finished.
HCVJA2000I Remediation has completed. (Pass Count: 1 / Failure Count: 0)
Manual system-reboot required.
HCVJA2042I System-reboot is necessary to continue. Please reboot the system manually.
OK
Cancel

Figure 8-41 Remediation handler interface for hotfix installation

Repeat this procedure for any other hotfix that you have defined as required in your security policy.

TCRMSServicePackInstallWinXpSp2

The *TCRMSServicePackInstallWinXpSp2* workflow is very similar to the one described above for the Windows Hotfix policy, as it installs a Microsoft Windows update as well. It is, however, a bigger and more serious one then a hotfix. The TCRMSServicePackInstallWinXpSp2 workflow was defined in the SERVICE_PACK_WF parameter in the Windows Service Pack policy to be used when the compliance check generated a FAIL or WARNING status. The purpose of the workflow is to install the missing service pack.

Downloaded from www.Manualslib.com manuals search engine

There is a small catch with this collector, as it is able to check for any Windows version service pack level including Windows NT, Windows XP, Windows 2000, and Windows 2003, but there is a possibility to specify only one remediation workflow. As we do not want to build one remediation package for all of the Windows versions, we have instructed the collector to only look for the Windows XP Service Pack 2 and named the remediation workflow after it. With this policy we check for an installed Windows XP Service Pack 2, so we must create an appropriate remediation workflow.

Follow the steps described below:

1. First open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

   ```
   cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
   bash
   cd $BINDIR/tcmremed/download
   mkdir TCRMSServicePackInstallWinXpSp2
   cd TCRMSServicePackInstallWinXpSp2
   ```

2. To build the package you must download the appropriate Service Pack 2 installation file from the Microsoft Web site. The Windows XP Service Pack 2 Network Installation Package for IT Professionals and Developers can be found at the following location:

   http://www.microsoft.com/downloads/details.aspx?FamilyId=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A&displaylang=en

   The file is named WindowsXP-KB835935-SP2-ENU.exe. Be warned that the size of this file is approximately 266 megabytes, so the download can take a few minutes depending on your network speed. Copy it to the newly created directory TCRMSServicePackInstallWinXpSp2.

3. Create the configuration file for the **s**putil.sh utility containing the instructions on how to build the package. Copy the Sample.properties file from the sample_TCRMSServicePackInstall_WinXpSp2Jp directory to the TCRMSServicePackInstallWinXpSp2 directory and edit it with the text editor to match the content specified in Example 8-13.

   Example 8-13 Sample.properties file for TCRMSServicePackInstallWinXpSp2 workflow

   ```
   WorkflowName=TCRMSServicePackInstallWinXpSp2

   AddRegistryValuesBeforeExecFlag=true

   AddRegistryValueBeforeExecParentKey.arrayLength=2
   AddRegistryValueBeforeExecKey.arrayLength=2
   AddRegistryValueBeforeExecName.arrayLength=2
   AddRegistryValueBeforeExecType.arrayLength=2
   ```


Downloaded from www.Manualslib.com manuals search engine

```
AddRegistryValueBeforeExecData.arrayLength=2

AddRegistryValueBeforeExecParentKey[0]=HKEY_LOCAL_MACHINE\\SOFTWARE\\Polici
es\\Microsoft\\WindowsFirewall
AddRegistryValueBeforeExecKey[0]=DomainProfile
AddRegistryValueBeforeExecName[0]=EnableFirewall
AddRegistryValueBeforeExecType[0]=dword
AddRegistryValueBeforeExecData[0]=0

AddRegistryValueBeforeExecParentKey[1]=HKEY_LOCAL_MACHINE\\SOFTWARE\\Polici
es\\Microsoft\\WindowsFirewall
AddRegistryValueBeforeExecKey[1]=StandardProfile
AddRegistryValueBeforeExecName[1]=EnableFirewall
AddRegistryValueBeforeExecType[1]=dword
AddRegistryValueBeforeExecData[1]=0

SourceFilename.arrayLength=1
ExeArg.arrayLength=1

SourceFilename[0]=WindowsXP-KB835935-SP2-ENU.exe
ExeArg[0].arrayLength=2
ExeArg[0][0]=/passive
ExeArg[0][1]=/norestart

RunQchainFlag=false

TmfWebUIEndpoint=tcmweb
```

4. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

   ```
   cd $BINDIR/tcmremed/download
   cd TCRMSServicePackInstallWinXpSp2
   $BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
   ```

5. Verify the result of running the tool with the following command:

   ```
   wlookup -ar SoftwarePackage | grep TCRMSServicePackInstallWinXpSp2
   ```

   If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number).

   ```
   TCRMSServicePackInstallWinXpSp2^1.0
   1406765930.1.851#SoftwarePackage::Spo#
   ```

This software package is large. The creation can take a while, and you should expect that it will consume more than 500 MB since it is stored twice — once in the $BINDIR\tcmremed\work directory and again on the HTTP server.

Downloaded from www.Manualslib.com manuals search engine

TCRZLSoftwareInstalled

The *TCRZLSoftwareInstalled* workflow is also very similar to the ones described above, as all it does is install software that is missing. The TCRZLSoftwareInstalled workflow was defined in the KEY_WF, VALUE_WF, and VALUE_DATA_WF parameters in the ZoneAlarm Software Installed policy to be used when the compliance check generated a FAIL or WARNING status.

The collector used to verify the ZoneAlarm firewall presence is the generic registry checking collector. Theoretically, you can call three different workflows if a registry key exists, if a value under this key exists, or if the value matches the specified rules. However, in our lab all three cases render the same result if the check fails, meaning that the software is not installed. So in all cases we must call the same workflow to download and run the ZoneAlarm installation package.

Similar to the Symantec Antivirus package, you need the installation media from the vendor to build that package, and you have to obtain the proper license.

Follow the steps described below:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

   ```
   cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
   bash
   cd $BINDIR/tcmremed/download
   mkdir TCRZLSoftwareInstalled
   cd TCRZLSoftwareInstalled
   ```

2. To build the package you must obtain the appropriate ZoneAlarm installation file from ZoneLabs. For testing purposes we use a 15-day trial version of the ZoneAlarm Pro installation file, which you can download from the ZoneLabs Web site at the following location:

   http://www.zonelabs.com/store/content/company/products/trial_zaFamily/trial_zaFamily.jsp?dc=12bms&ctry=US&lang=en&lid=db_trial

   You can easily modify the policy to check for any other software and workflow to install it when missing. During the time of writing this book the version available on the Web was 6.5.737. If you have downloaded the ZoneAlarm Pro trial or you are in possession of a fully licensed installation image, copy the installation package to the TCRZLSoftwareInstalled directory.

Downloaded from www.Manualslib.com manuals search engine

3. Create the configuration file for the sputil.sh utility containing the instructions on how to build the package. Copy the Sample.properties file from the sample_TCRZLSoftwareInstalled directory to the TCRZLSoftwareInstalled directory and edit it with the text editor to match the content specified in Example 8-14.

Example 8-14 Sample.properties file for TCRZLSoftwareInstalled workflow

```
WorkflowName=TCRZLSoftwareInstalled

SourceFilename.arrayLength=1
ExeArg.arrayLength=1

SourceFilename[0]=zapSetup_65_737_000_en.exe
ExeArg[0].arrayLength=3
ExeArg[0][0]=/s
ExeArg[0][1]=/i
ExeArg[0][2]=/noreboot

TmfWebUIEndpoint=tcmweb
```

4. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

```
cd $BINDIR/tcmremed/download
cd TCRZLSoftwareInstalled
$BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
```

5. Verify the result of running the tool with the following command:

```
wlookup -ar SoftwarePackage | grep TCRZLSoftwareInstalled
```

If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number).

```
TCRZLSoftwareInstalled^1.0      1406765930.1.852#SoftwarePackage::Spo#
```

You may notice the three arguments passed with the ZoneAlarm installation file, which are flags /s /i /noreboot. They are explained below:

/i This means that the software must be installed.

/s This means that the process of installing/uninstalling must be silent, so there is no pop-up asking for user input.

/noreboot This means that the workstation should not automatically reboot after the installation.

Depending on the technology, the installer for any particular software may use the flags in a different way, but we strongly recommend that the remediation

Downloaded from www.Manualslib.com manuals search engine

workflows installing or uninstalling software should use silent mode whenever possible.

TCRZLSoftwareRunning

The *TCRZLSoftwareRunning* workflow was defined in the SERVICE_RUNNING_WF parameter in the ZoneAlarm Software Active policy to be used when the compliance check generated a FAIL or WARNING status. This is one of the two workflow types called by the nac.win.any.services.PostureService collector. It is executed during the remediation of the violation when a service that should be running is stopped.

To build the remediation package:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create the directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRZLSoftwareRunning
cd TCRZLSoftwareRunning
```

2. Create the very simple Windows batch file named startupTrueVectorService.bat, which contains only one line, as shown below:

```
net start "TrueVector Internet Monitor"
```

   Copy this batch file to the TCRZLSoftwareRunning directory.

3. Create the configuration file for the sputil.sh utility containing the instructions about how to build the package. Copy the Sample.properties file from the sample_TCRZLSoftwareRunning directory to the TCRZLSoftwareRunning directory and edit it with the text editor to match the content specified in Example 8-15.

Example 8-15 Sample.properties file for TCRZLSoftwareRunning workflow

```
WorkflowName=TCRZLSoftwareRunning

CorequisiteFilesFlag=true

SourceFilename.arrayLength=1
ExeArg.arrayLength=1

SourceFilename[0]=startupTrueVectorService.bat
ExeArg[0].arrayLength=0

TmfWebUIEndpoint=tcmweb
```


Downloaded from www.Manualslib.com manuals search engine

4. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

```
cd $BINDIR/tcmremed/download
cd TCRZLSoftwareRunning
$BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
```

5. Verify the result of running the tool with the following command:

```
wlookup -ar SoftwarePackage | grep TCRZLSoftwareRunning
```

   If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number):

```
TCRZLSoftwareRunning^1.0     1406765930.1.843#SoftwarePackage::Spo#
```

TCRMessengerDisabled

The *TCRMessengerDisabled* workflow was defined in the SERVICE_DISABLED_WF parameter in the Messenger Service Disabled policy to be used when the compliance check generated a FAIL or WARNING status. This is the second type of the two workflows called by the nac.win.any.services.PostureService collector. It is called during the remediation of a violation when the service that should be disabled is not.

To build the remediation package follow the steps described below:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then create a directory for the workflow files. To do this issue the following commands:

```
cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
bash
cd $BINDIR/tcmremed/download
mkdir TCRMessengerDisabled
cd TCRMessengerDisabled
```

2. Create the very simple Windows batch file named disableMessengerService.bat, which contains only one line shown below:

```
sc config Messenger start= disabled
```

   Important: Make sure that there is no space between the word `start` and the equals sign (`=`). Also make sure there is a space between `start=` and the word `disabled`.

   Copy this batch file to the TCRZLSoftwareDisabled directory.

3. Create the configuration file for the sputil.sh utility containing the instructions on how to build the package. Create the Sample.properties file in the

Downloaded from www.Manualslib.com manuals search engine

TCRZLSoftwareDisabled directory and edit it with the text editor to match the content specified in Example 8-16.

Example 8-16 Sample.properties file for TCRMessengerDisabled workflow

```
WorkflowName=TCRMessengerDisabled

CorequisiteFilesFlag=true

SourceFilename.arrayLength=1
ExeArg.arrayLength=1

SourceFilename[0]=disableMessengerService.bat
ExeArg[0].arrayLength=0

TmfWebUIEndpoint=tcmweb
```

4. Run the **sputil.sh** command to create the software package block and publish it on the Web Gateway. To achieve this run the following commands:

   ```
   cd $BINDIR/tcmremed/download
   cd TCRMessengerDisabled
   $BINDIR/tcmremed/bin/sputil.sh -p Sample.properties
   ```

5. Verify the result of running the tool with the following command:

   ```
   wlookup -ar SoftwarePackage | grep TCRMessengerDisabled
   ```

   If the package was created the result will look like below (the number in the middle of the resulting string will be different in your environment as it is meant to be unique and is associated with Tivoli Management Region number).

   ```
   TCRMessengerDisabled^1.0     1406765930.1.855#SoftwarePackage::Spo#
   ```

This concludes the creation of remediation packages required for automatic remediation of noncompliant clients.

8.4.1 Modification of the remediation packages

Modification of published remediation packages is a part of normal life-cycle operations for a security policy and related remediation processes. With the current version of the solution, versioning of packages in not supported. In order to modify the package you must remove it and then create and publish a new one.

Downloaded from www.Manualslib.com manuals search engine

In order to remove the package for the TCRMessengerDisabled remediation workflow:

1. Open a command prompt, import the environment variables for the Tivoli Framework, and start bash. Then go the directory for the TCRMessengerDisabled workflow. To do this issue the following commands:

   ```
   cmd /k %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
   bash
   cd $BINDIR/tcmremed/download
   cd TCRMessengerDisabled
   ```

2. Copy the file TCRMessengerDisabled_publish.sh to a new one, name it `TCRMessengerDisabled_unpublish.sh`, and open it with a text editor to change the content:

   a. Change `-publish` to `-unpublish`.
   b. Remove the `-i all` option.

   The final content should look like Example 8-17.

Example 8-17 Content of TCRMessengerDisabled_unpublish.sh script

```
wweb -unpublish -p
/TCRMessengerDisabled/nac.win.any.services.PostureServices/SERVICE_DISABLED_WF/latest -v 1.0 -w
tcmweb -f @SoftwarePackage:"TCRMessengerDisabled^1.0"#tcmweb-region
```

3. Run the new script to remove the package from the Web Gateway server:

   ```
   ./TCRMessengerDisabled_unpublish.sh
   ```

4. Remove the package from Tivoli Configuration Manager with the following command:

   ```
   wdel @SoftwarePackage:"TCRMessengerDisabled^1.0"
   ```

5. Modify the content of the package and run the sputil.sh utility to recreate the package as described in “TCRMessengerDisabled” on page 435.

8.5 Conclusion

This concludes all three sections for our ABBC project implementation. At this point you are ready to deploy your pilot environment and collect your own experiences.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Part 3

Appendixes

In the following two appendixes we take a closer look at these topics:

- General hints and tips for everything around the IBM Integrated Security Solution for Cisco Networks
- A generic introduction to the Cisco Network Admission Control initiative (provided by Cisco)

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

A

Hints and tips

This appendix contains hints, tips, and other useful information that can help the implementer to have a better understanding of the IBM Integrated Security Solution for Cisco Networks. It also describes the NAC Appliance offering and presents a working prototype for integration with the NAC Appliance offering.

Information provided in this section may also be used for problem determination and detailed analysis of the key components and associated sequence diagrams.

This section includes:

- Deployment overview
- Top-level sequence of events
- Security Compliance Manager and NAC compliance subsystem
- Cisco NAC sequence of events
- Fault isolation
- Security Compliance Manager server and client
- Tools and tricks

Note: For more detailed troubleshooting procedures you should consult the individual product documentation.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Deployment overview

The solution deployment starts with the registration of a set of attributes for the IBM Integrated Security Solution for Cisco Networks on the Cisco Secure ACS server, as shown in Figure A-1 on page 443. This registration describes the type of data that will be passed to the ACS by the Tivoli Compliance and Remediation subsystems. Currently. two IBM attributes are registered with ACS: *PolicyVersion* and *ViolationCount*.

Next, a policy is installed on the client. This policy is created on the Security Compliance Manager server but for the purposes of troubleshooting, this is transparent to the client. It is the installed *policy* on the client that is of interest. Note that when a new policy is installed a new set of *collector objects* will be placed in the%SCM_HOME%/.client/collectors directory. These collectors determine what data the client will collect.

The Configuration Manager server is also loaded with *remediation* (or *software*) *artifacts*, which are the objects of code that will be used to effect remediation on the clients. Examples of these artifacts would be self-installing updates, updated definition files, updated policy files, and so on.

After the solution has been configured with these objects, the NAC process is started. The following sequence diagrams provide a detailed description of the timing and events that happen during a typical NAC admission procedure.

In Figure A-1 on page 443, the shadowed boxes represent files or content that is imported or modified to change the behavior of the deployment. The heavily lined boxes represent software that is installed as part of the deployment.

Downloaded from www.Manualslib.com manuals search engine

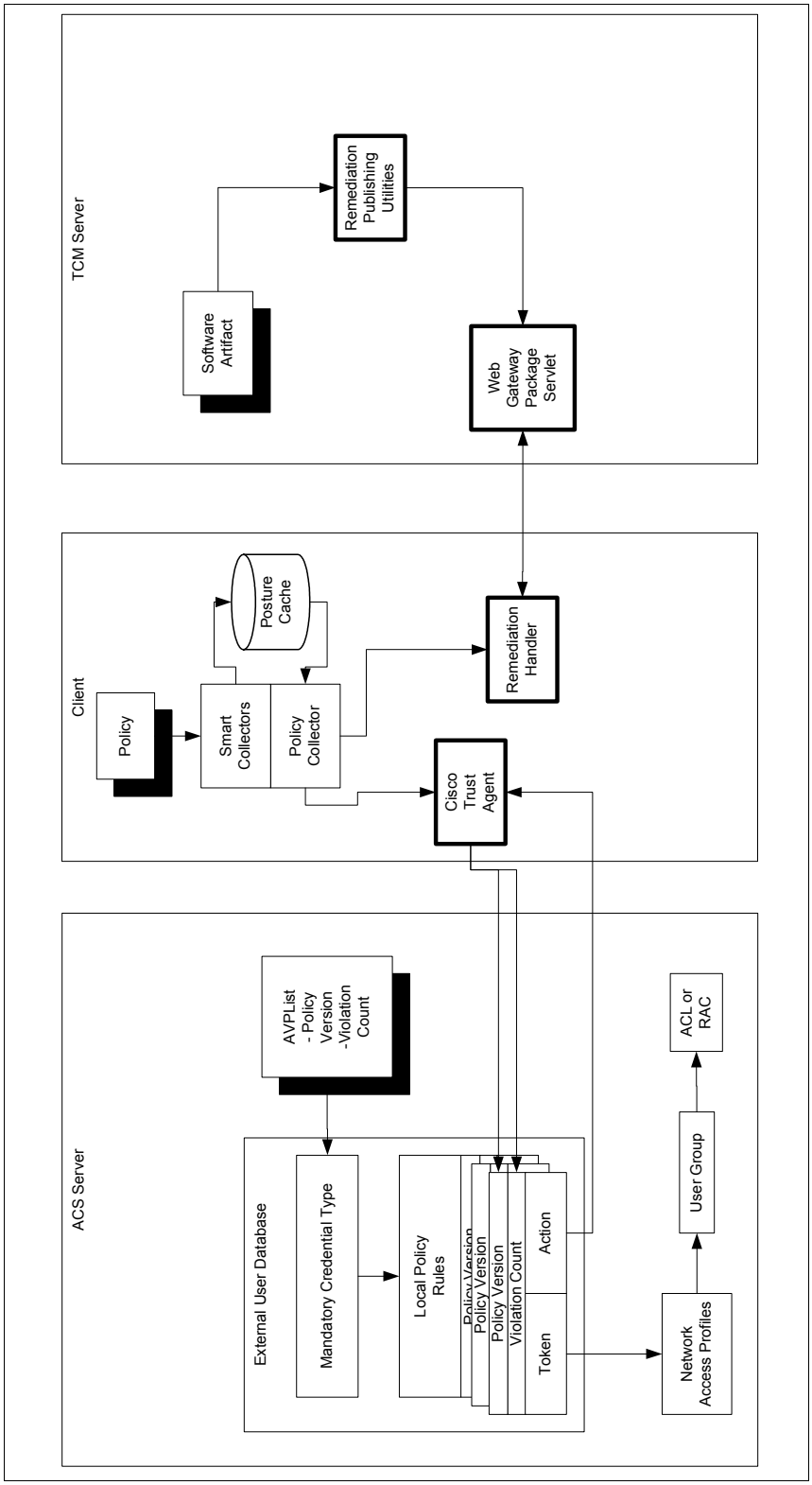


Figure A-1 TRC-specific objects and relationship

Downloaded from www.Manualslib.com manuals search engine

Top-level sequence of events

The NAC process starts when the client tries to access a protected network. When the Network Access Device (typically a switch or router) recognizes that a client is attempting access, it issues a PostureQuery request to the client asking the client to report its posture. The posture message is passed via the Cisco Trust Agent to the Security Compliance Manager policy collector, which responds with a PolicyVersion and a ViolationCount, the two attributes that have been registered with the ACS for the use of client remediation. The values passed along for these attributes are considered to define the client's posture.

When the ACS has received the posture attributes from the client, it computes these against defined policies and computes a posture (or posture token) for the client. The two postures that are typically used are *Quarantine* and *Healthy*. The ACS sends a PostureNotification to the client; if the client is healthy, that is the end of the NAC process. If the client is quarantined, then the notification also includes an action, which is the URL to be used to request automated remediation. In either case, the Cisco Trust Agent pops up a window on the client that displays the current posture.

If a quarantine PostureNotification is received by the client, it will pass all of the known remediation information in the posture cache to the remediation handler, which includes a pop-up GUI that enables the user to see what the state of compliance is and to manually address any problems that are reported. The remediation handler UI includes a fully functional Web browser, and HTML content can be customized for policies to provide users with directions or links to Web sites where they can download remediation content. The remediation handler also includes several buttons for the user to select the desired behavior:

- The Rescan button forces an immediate rescan by all of the collectors, and all of the data in the local posture cache is updated. This completes the current process, and the client will wait for the network to poll it for changes, at which time the process will be started again.
- The Fix Now button initiates the automated remediation process.

The sequence diagram shown in Figure A-2 on page 445 shows the sequence of events for the automated remediation process at the highest level.

Downloaded from www.Manualslib.com manuals search engine

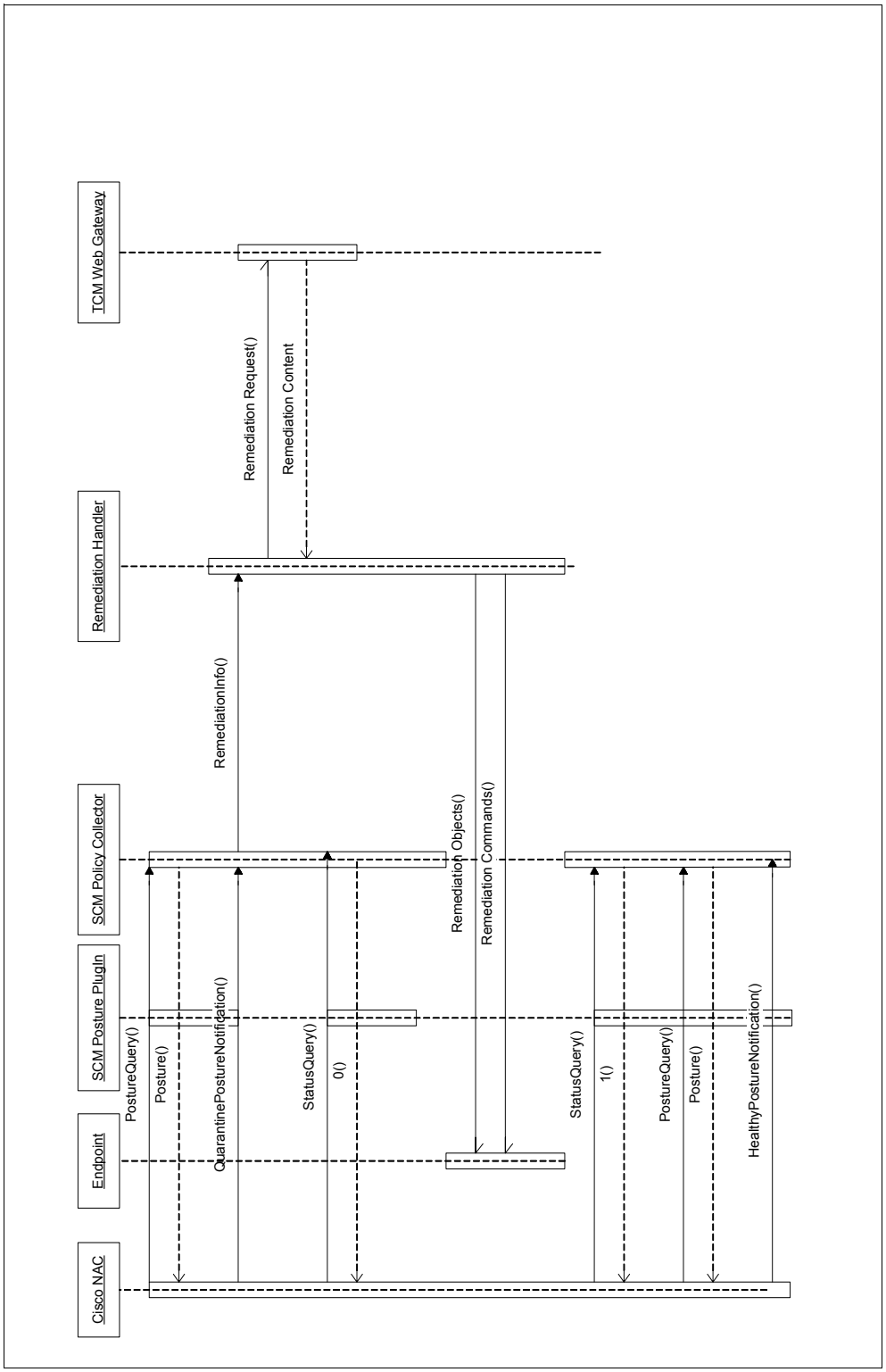


Figure A-2 ISSCN top-level sequence diagram

Downloaded from www.Manualslib.com manuals search engine

Security Compliance Manager and NAC compliance subsystem

Figure A-3 shows the compliance subsystem and data flow between the subcomponents that can help during problem determination and also provides insight to better understand the interactions between the modules.

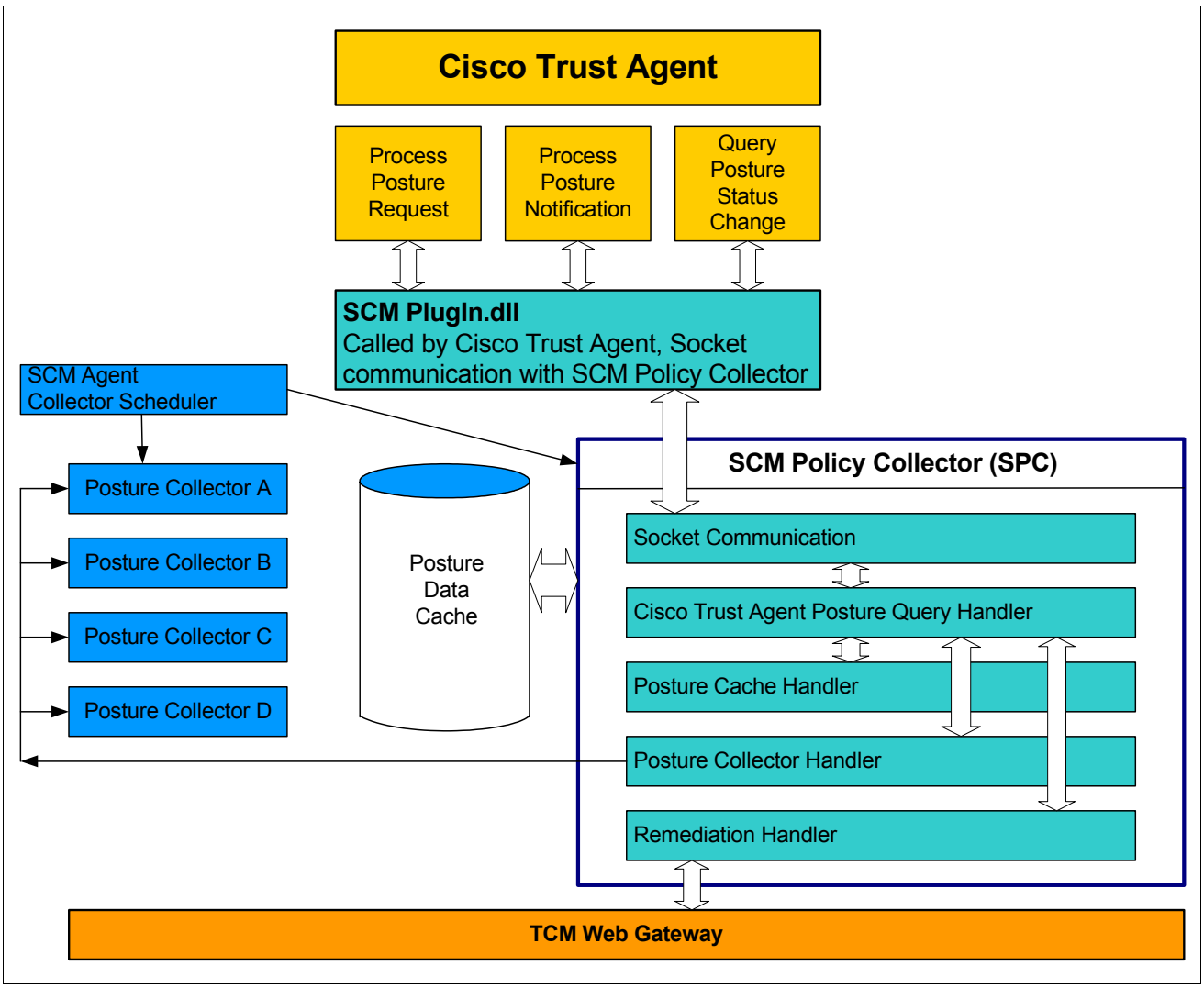


Figure A-3 The compliance subsystem

Downloaded from www.Manualslib.com manuals search engine

Cisco NAC sequence of events

The NAC process is initiated by the network. Whenever access to a protected network is detected, the Network Access Device queries the endpoint for its posture. In addition, there are two polling cycles that control what requests are sent to the client by the network and when. There are three basic messages that the network can send to the client: Two of these are queries (PostureQuery and StatusChangeQuery) and one is a notification (PostureNotification).

Figure A-4 shows the communication flow between the Cisco Trust Agent and the Security Compliance Manager agent.

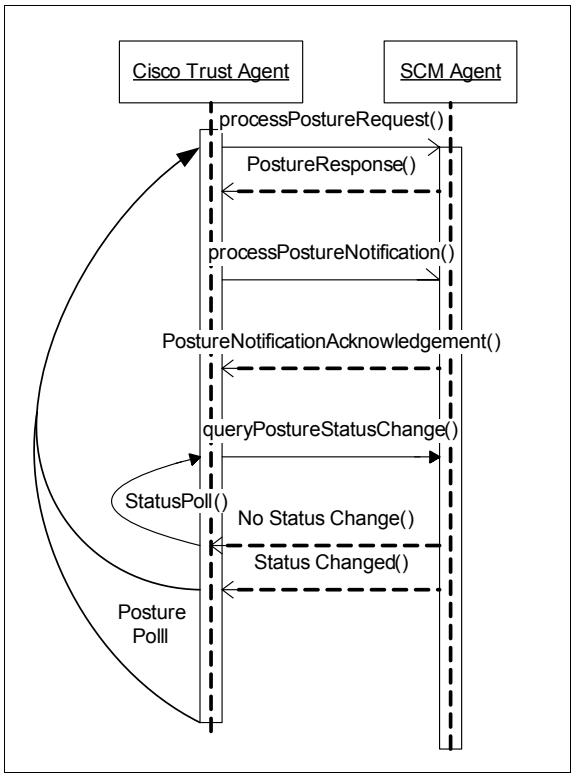


Figure A-4 Cisco NAC sequence diagram

The PostureQuery asks the client for the full set of attribute data that the client has registered with the ACS. The client responds to the PostureQuery by sending the applicable values (PolicyVersion and ViolationCount) based on the data in the local policy cache.

The StatusChangeQuery asks whether there has been a change in state since the last PostureQuery or StatusChangeQuery. Both of these queries have their own polling cycle configured on the Network Access Device. It is typical for the PostureQuery polling cycle to be set to a relatively high value so that any

Downloaded from www.Manualslib.com manuals search engine

attempts by the client to access a protected resource will also trigger a PostureQuery from the network. This StatusQuery cycle is typically configured to a low value so that any changes that occur on the client after it has been admitted to the network will be detected quickly.

In a typical scenario, the network initiates the process by sending a PostureQuery to the client. The client responds with its current posture attributes, which are then compared against configured rules on the ACS Server. Based on this comparison, the client will be evaluated as either Healthy or Quarantined:

- In the simpler case, the client is evaluated as healthy and a notification of heathy evaluation is sent to the client. Note that this notification is *not* the PostureNotification that would be sent to the client if the posture was evaluated as quarantined.

  The healthy notification is processed completely by the Cisco Trust Agent on the client and the Tivoli Compliance and Remediation client never sees it. After this notification is sent, the network enters the StatusQuery polling cycle, basically asking the client whether anything has changed each time the cycle repeats. If something changes on the client, it will be reflected as a status change and the network will then reset both polling cycles and issue a PostureQuery to the client, starting the whole process over to evaluate the new state on the client.

- If the initial PostureQuery ends with the client being evaluated as quarantined, this status is sent to the client as a PostureNotification, which is accompanied by a URL that the client uses to request remediation. The client responds by acknowledging the PostureNotification, signaling the network to enter the StatusQuery polling cycle. The network continues to poll for state changes on the client using the StatusChangeQuery request. Now the client is free to request automated remediation or to prompt the user to manually remediate whatever violations have been detected.

  The system stays in this state until remediation actions are complete, at which time the Security Compliance Manager Client will automatically rescan all collectors, or until the user presses the Rescan button on the remediation handler. Either of these events cause a rescan of all collectors, and if anything has been remediated on the client, the state changes. The next time the network polls, it realizes that the status has changed and re-initiates the process by issuing a PostureQuery to the client.

Fault isolation

Now that the overall sequence of events is understood, it should be straightforward to isolate any fault to one of the subsystems or interfaces and

Downloaded from www.Manualslib.com manuals search engine

then to determine the actual problem based on the expected behavior of the solution.

Assuming that all of the software has been installed and is running, when the client first tries to connect to a protected network, it should receive a pop-up message from the Cisco Trust Agent stating either that the client is healthy or that the client has been quarantined.

If no message appears, either the Cisco Trust Agent is not running on the client (check the Windows services panel for the Cisco Trust Agent) or the Network Access Device is not seeing the client. Also be sure that the host's personal firewall and the NAD configuration allow pings. An easy way to check out this situation is to **`ping`** a host in the protected network.

- If the pings are successful, then the client should either have received a "healthy" message or the NAD may be configured to allow clientless devices (for example, with no Cisco Trust Agent running) access.
- If the pings time out (Request Timed Out) then the NAD is not performing correctly.
- If the pings fail with a *Destination Unreachable* message, then the NAD is quarantining the host and the Cisco Trust Agent is probably not running.

If a message appears, then the NAD and the Cisco Trust Agent are communicating correctly.

If a client is quarantined, then the remediation handler (the Security Compliance Manager pop-up GUI) should display all of the violations along with the options to Rescan, Fix Now, or Close:

- Any manual remediation actions should be followed with Rescan to cause any state changes to be detected, and the next time the network polls with a StatusQuery, the state change will cause a full PostureQuery and the evaluation process will be restarted.
- Fix Now requests automated remediation and initiates the remediation events.
- Close simply closes the remediation handler.

When Fix Now is clicked, the automated remediation process starts.

At this point, the remediation handler requests remediation from the Tivoli Configuration Manager Web Gateway via the SoftwarePackageServlet application that is installed on the server. The remediation information passed by the client is analyzed by this servlet and the relevant remediation objects are sent to the client. The remediation handler then manages the installation and execution of these remediation objects and then triggers a rescan of the

Downloaded from www.Manualslib.com manuals search engine

collectors, at which time any state changes affected by the remediation process will be discovered. The next time the network polls for StatusChange, it will receive a `true` response and will request the new posture data to evaluate against the existing policy.

Details about this process can be found in the Security Compliance Manager Client's client.log file and several log files on the Web Gateway, including the HTTP Server component's access.log and the application-specific logs on the WebSphere Application Server.

Security Compliance Manager server and client

Figure A-5 illustrates Tivoli Security Compliance Manager client/server communication and the interaction between the server and client and associated TCP port numbers.

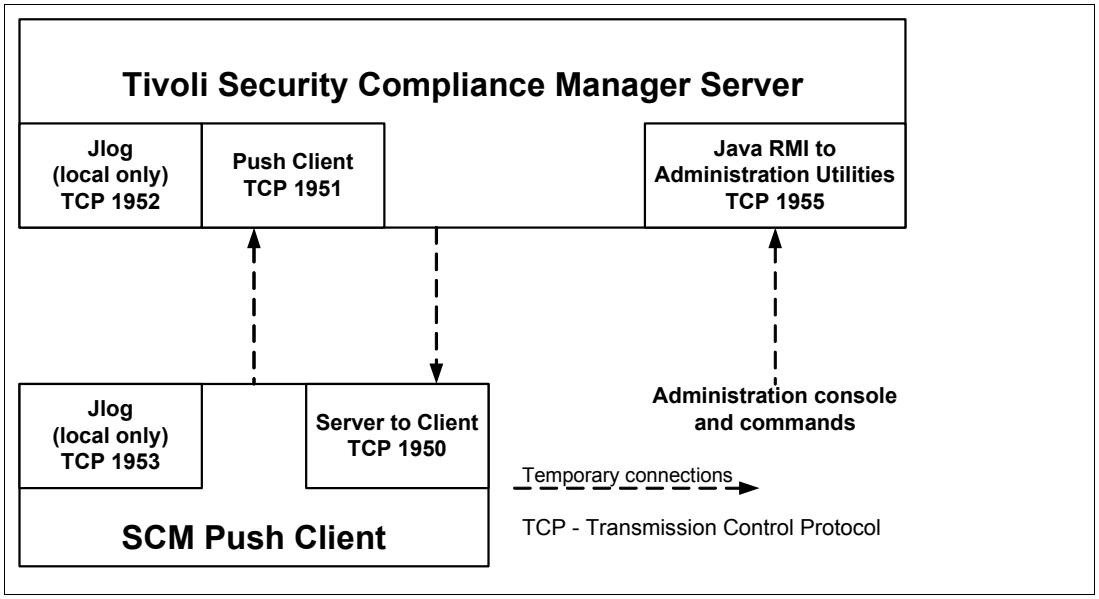


Figure A-5 Communication port usage in Security Compliance Manager server and client

Figure A-5 shows the default port usage for Tivoli Security Compliance Manager. The direction of the arrows in the diagram indicate the initiator of the communication. For example, communication from the server to a push client is initiated by the server on port 1950. Similarly, communication from a push client to the server is initiated by the client on port 1951.

Downloaded from www.Manualslib.com manuals search engine

Communication port usage

Tivoli Security Compliance Manager server and client communicate only with temporary connections. A persistent connection is not required because the Security Compliance Manager/NAC concept can function without the Security Compliance Manager server after the client policies are deployed.

Communications among Tivoli Security Compliance Manager components are secured using 128-bit Secure Sockets Layer (SSL) encryption. The cipher suites that are used are RSA_WITH_RC4_128_SHA, RSA_WITH_RC4_128_MD5, and RSA_WITH_3DES_EDE_CBC_SHA.

Communication occurs using the Transmission Control Protocol (TCP) port numbers specified during the installation of the server and the clients. Communication between the clients and the server is performed using an internal protocol.

Communications between the administration utilities and the server are handled using the Java Remote Method Invocation (RMI) technology.

Summary of default port usage

- Communications between the server and a push client:
  - Server to client: TCP 1950
  - Client to server: TCP 1951
- Communications between the server and the administration console or administration commands and administration utility:
  - Server: TCP 1955 (RMI-naming) administration utility

Tools and tricks

This section includes some useful commands that can assist in troubleshooting and problem determination.

Note: These commands are listed mainly to assist in resolving problems in a NAC setup; for any additional information about these or other commands, you should refer to the Cisco product guides.

Cisco NAC

The following Cisco router commands and other useful information about the ACS server, which are unique to Network Admission Control, are provided below.

Downloaded from www.Manualslib.com manuals search engine

Cisco IOS Software router

On a Cisco router running Cisco IOS Software, these commands are useful for debugging:

show eou	Shows eou (EAPoverUDP) settings including polling cycle timeouts.
show eou all	Shows current eou cache data.
eou logging	Turns on eou logging output.
eou reval ip xx.xx.xx.xx	Forces immediate revalidation of client with IP address xx.xx.xx.xx.
clear ip admission cache *	Clears the IP admission cache for all clients (forced revalidation of all clients).

Cisco IOS Software switch

For Cisco switches configured for IP-based NAC, the commands listed in the preceding section apply to both a router and a switch. For 802.1x-based NAC a useful command is the following. (NAC values are in bold at the bottom of the output.)

show dot1x interface (interface) details

```
Dot1x Info for FastEthernet1/0/10
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = (From Authentication Server)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 000c.2929.25cd
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED
ReAuthPeriod              = 60

ReAuthAction              = Reauthenticate
```


Downloaded from www.Manualslib.com manuals search engine

```
TimeToNextReauth          = 48
Authentication Method     = Dot1x
Posture                   = Healthy
Authorized By             = Authentication Server
Vlan Policy               = 10
```

Cisco Secure ACS server

On a Cisco Secure ACS server Web GUI, go to the reports section and look at the Passed Authentications and Failed Attempts reports.

The Failed Attempts report shows instances where the NAC process was not completed successfully for some reason. The Authentication Failure Code column gives an indication of what failed. Use this report to find details about why NAC challenges are not completing. This typically leads to something amiss in your Cisco NAC setup, between the Cisco Trust Agent, Cisco IOS Software NAD, and Cisco Secure ACS.

The Passed Authentications report shows NAC challenges that were completed successfully, even if the result was that the client was quarantined. If entries are being added to this report, your basic Cisco NAC setup is probably good and the hosts are being quarantined due to their compliance postures. At any rate, you can see the values that are passed from the Security Compliance Manager Posture Plug-in for each host in this report.

Cisco Trust Agent

On the client, the Cisco Trust Agent handles all communications with the Cisco network. The accompanying file, ppta.exe, can be used to query the Cisco Trust Agent to see what information it is passing to the network. This file should be placed into the %CTA_HOME% directory and executed from there. When run, it pops up a window. Click the **Update List** button to display all of the registered Posture Plug-ins on the system. You should see the IBM Security Compliance Manager plug-in displayed in the list. Select the IBM plug-in and click the **Posture** Button. The attributes and values that are passed to the network by the IBM plug-in are displayed in the lower window. Make sure that these values are the expected values.

Tools and tricks for the client

The information in this section is useful for problem determination and the proper installation of the Security Compliance Manager client.

Note: You might check Tivoli user documentation and product release notes for any additional commands or information. Commands shown below are best aimed at providing comprehensive hints and tips for this concept.

Downloaded from www.Manualslib.com manuals search engine

Security Compliance Manager client

When the Security Compliance Manager client is started, the Security Compliance Manager policy collector should listen for TCP connections on *port 40500*.

If a **netstat -an** command is run in a command window, you should see this line:

```
TCP    127.0.0.1:40500        0.0.0.0:0              LISTENING;
```

If this line does not appear in the list of connections, then the Security Compliance Manager client policy collector is not running correctly.

If the client is listening on port 40500, you can **telnet** to the client and issue the same commands that the Cisco Trust Agent would issue. This technique should be used when you have to troubleshoot the interface between the Cisco Trust Agent and the Security Compliance Manager policy collector.

In a command line window, issue the **telnet localhost 40500** command to establish a connection with the client.

With the following commands, you can see what is being passed back to the network, look at the complete posture cache, and test calls to the remediation handler.

The commands **pquery** and **pstatuschange** have no arguments. **pquery** displays the current value of all defined posture attributes.

Note: When you issue a **pquery** command, the next time the network issues a **pstatuschange** it will receive a *false* response. If you issue a **pquery** command, you should clear the client's cache on the router or initiate a rescan of the client on the router.

The **pstatuschange** command displays either true or false, reflecting how the network determines whether the client's status has changed since the last **pquery**.

The **print** and **runall** commands display and refresh the posture cache. **print** shows the complete contents of the posture cache and is useful to see what the client sees as the state of your system. **Runall** runs all of the collectors again and refreshes the posture cache with fresh information.

The **pnotify <REM_URL>** command starts the remediation handler, with <REM_URL> being the URL of the remediation listener that can be called to handle the remediation request.

Downloaded from www.Manualslib.com manuals search engine

Client logging can be turned on by setting the debug property to `true` in the %SCM_HOME%\client\client.pref file. When turned on, a file called client.log is created and updated in the %SCM_HOME/client directory. This file displays any notification received from the network.

Remediation handler

When the Security Compliance Manager client is started, it automatically starts the remediation handler. Log messages from the remediation handler appear in the Security Compliance Manager Client's client.log file.

NAC Appliance details

Note: NAC Appliance is also referred to as Cisco Clean Access, and most of the references and figures in this section use the Clean Access naming.

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager Web console and enforced through the Clean Access Server and the Clean Access Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation before clients access the network.

Cisco NAC Appliance components

The following is a list of the NAC Appliance components.

- Clean Access Manager (CAM)

  This is the administration server for Clean Access deployment. The secure Web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment. For Out-of-Band (OOB) deployment, the Web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP. (Note that the CAM Web admin console supports Internet Explorer® 6.0 or later only, and requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for Web login and Clean Access Agent authentication.)

- Clean Access Server (CAS)

  Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM Web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Clean Access system requirements. It can be deployed in-band (always inline with user traffic) or out-of-band (inline with user traffic only during authentication/posture

Downloaded from www.Manualslib.com manuals search engine

assessment). It can also be deployed in Layer-2 mode (users are L2-adjacent to CAS) or Layer-3 (users are multiple L3 hops away from the CAS) mode.

- Clean Access Agent (CAA)

  This ia a read-only agent that resides on Windows clients. The Clean Access Agent checks applications, files, services, or registry keys to ensure that clients meet your specified network and software requirements prior to gaining access to the network. (Note that there is no client firewall restriction with Clean Access Agent vulnerability assessment. The Agent can check the client registry, services, and applications even if a personal firewall is installed and running.)

- Clean Access Policy Updates

  These are regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software.

In-band versus out-of-band

Customers often ask which deployment modes are most appropriate for their networks. In fact, an organization can deploy both, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for wired users, for example). The Cisco Clean Access Manager is designed to support both in-band and out-of-band Cisco Clean Access servers, as well as the switches associated with the out-of-band portion of the network.

With the Cisco Clean Access in-band deployment, the Clean Access Server is always inline with user traffic — before, during, and after authentication, posture assessment, and remediation. The server can be used to securely control authenticated and unauthenticated user traffic by managing traffic policies based on protocol/port or subnet, providing bandwidth policy management based on shared or per-user, or using time-based sessions and heartbeat controls. In-band deployment supports any edge access device as long as the MAC address and IP address of the client machine are visible to the Clean Access Server. Because the server is in-band with traffic, the in-band deployment mode is ideal for environments with the following characteristics:

- Shared media ports
- Bandwidth throttling by role required
- Wireless access points
- Voice over IP (VoIP) phones
- Network infrastructure built with products other than Cisco products

In an out-of-band deployment of Cisco Clean Access, the Clean Access Server is in-band only during the process of authentication, posture assessment, and remediation. Once the user's device has successfully logged on, its traffic then bypasses the Clean Access Server and traverses the switch port directly. In the

Downloaded from www.Manualslib.com manuals search engine

meantime, the Clean Access Manager provides port-level or role-level control by assigning ports to specific VLANs, assigning users to specific roles that map to specific VLANs, and providing a time-based session time out per role. Cisco Clean Access out-of-band is most appropriate for high-throughput, highly routed environments such as campuses, branch offices, and extranets. It is not suitable for use with shared media devices, such as hubs and wireless access points. The out-of-band deployment mode is ideal for environments with the following characteristics:

- Healthy user traffic does not flow through CAS.
- Posture-based VLAN segmentation.
- Voice over IP (VoIP) phones.

NAC Appliance integration

At the time of writing, Cisco is offering two separate Network Admission Control solutions: NAC Framework and NAC Appliance. Applications that are compatible with NAC Framework do not work with NAC Appliance, as the interfaces are currently dissimilar. Cisco has stated their intention to make NAC Framework and NAC Appliance solutions compatible, but at the current time this is not the case. Most of the content of this publication up to this point has been relevant to the NAC Framework, but does not necessarily apply to NAC Appliance.

However, NAC Appliance has been deployed by a larger set of customers than NAC Framework simply due to its lower cost factor and deployment footprint. In order to provide Cisco NAC Appliance customers access to the compliance and remediation capabilities that we currently provide for NAC Framework, this integration has been prototyped to prove the concept. This integration is designed to provide an easy migration from NAC Appliance to NAC Framework solutions as customers expand their NAC deployments. In fact, with this design the Tivoli Compliance and Remediation solution can be simultaneously deployed with both NAC Framework and NAC Appliance if so desired. This allows customers to develop compliance policies and remediation objects for the Tivoli subsystems, and that investment will be protected regardless of which alternative they select.

This section describes the integration of the current Tivoli Compliance and Remediation components with NAC Appliance. Many of the components used to perform this integration are not in production at the time of this writing and hence are not currently supported. However, this integration delivers an automated remediation capability and the ability to monitor clients after they have been admitted to the network. The value that these features add to a NAC Appliance solution is significant enough to warrant the description of this integration herein, with the expectation that production-quality versions of these components will become generally available.

Downloaded from www.Manualslib.com manuals search engine

Interested parties can use this design and the prototypes of these components to perform this integration in labs, for demos, and training purposes.

Integration design

The fundamental premise of this integration is for Security Compliance Manager to validate the compliance posture of the endpoint and indicate the state of the client by managing the state of a well-known file on the client and for NAC Appliance to admit an endpoint to the network based on the existence of this file. In addition, NAC Appliance will verify that the Security Compliance Manager client is running on the endpoint.

NAC Appliance is inherently capable of checking for services running on clients and for the existence of specific files on clients. These capabilities are used to validate that the Tivoli Security Compliance Manager Client is running and check that a special compliance semaphore file indicating the compliance state of the endpoint exists in order to admit the endpoint. A special NAC Appliance Agent is installed on the client for this integration, and if either of the requirements is not met, it will run a specific executable on the client.

Note: The NAC Appliance Version 4.1 (availability date September 19, 2006) will have a *Qualified Executable Launch* that will eliminate the need for the special agent in this scenario.

Security Compliance Manager can have a prototype version of the policy collector installed that will manage the existence of the compliance semaphore file based on the client's compliance status. This special version of the policy collector updates this file whenever a posture scan is performed. In addition, if the client is connected to the protected network and a compliance violation occurs, this special policy collector will initiate an HTTPS request to the NAC Appliance Manager that terminates the client's admission session and forces the client to restart the admission process.

Downloaded from www.Manualslib.com manuals search engine

A high-level overview of this design is depicted in Figure 8-42.

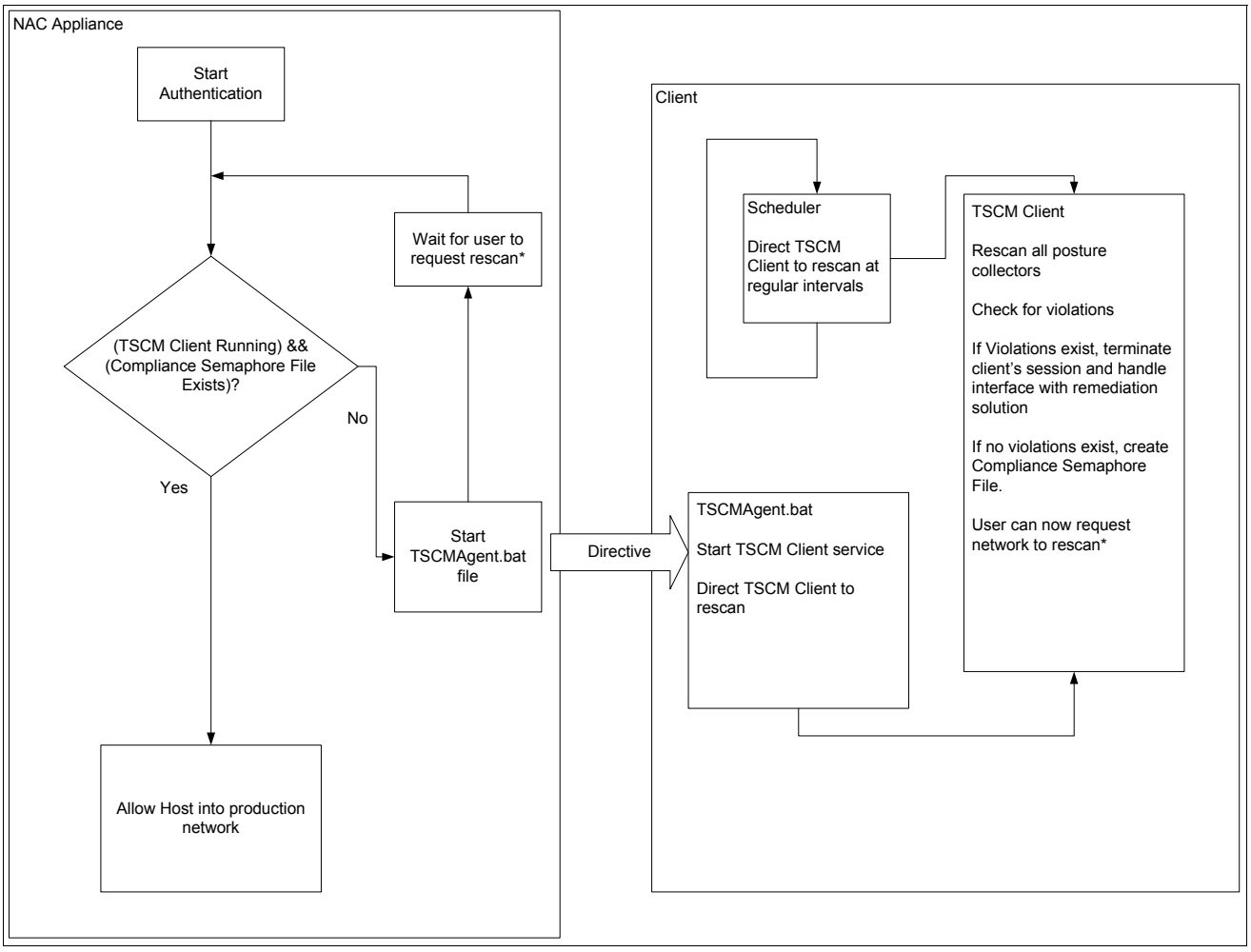

NAC Appliance
Start Authentication
Wait for user to request rescan*
(TSCM Client Running) && (Compliance Semaphore File Exists)?
No
Yes
Start TSCMAgent.bat file
Allow Host into production network
Directive
Client
Scheduler
Direct TSCM Client to rescan at regular intervals
TSCM Client
Rescan all posture collectors
Check for violations
If Violations exist, terminate client's session and handle interface with remediation solution
If no violations exist, create Compliance Semaphore File.
User can now request network to rescan*
TSCMAgent.bat
Start TSCM Client service
Direct TSCM Client to rescan

Figure 8-42 High-level overview

Integration components

The following components are to be considered prototypes for use in labs, demos, training classes, and similar purposes. They are implemented in an insecure manner to allow interested parties to better understand how this integration works.

NAC Appliance Agent

This specially built agent is customized to run the TSCMAgent.bat file whenever the required compliance state is not met on the client. When the production version of this file is delivered, it will not run a .bat file, but will require a signed executable.

Downloaded from www.Manualslib.com manuals search engine

TSCMAgent.bat

This script creates the compliance semaphore file in and intermediate state that indicates that the client is in the admission process. It then starts the TSecurity Compliance Manager Client service. These are the two conditions that should be checked for in any NAC Appliance policy created for this integration. Finally, it runs the TSecurity Compliance Manager Client's statuscheck.exe, which forces the TSecurity Compliance Manager Client to run a rescan and recompute the compliance posture.

NACApplianceCompliance.entry

This file is an identical copy of the compliance semaphore file in an intermediate state that indicates that the client is in quarantine. It is used by the TSCMAgent.bat file to create the actual semaphore file to indicate this state to the policy collector.

Policy collector

This specially built policy collector has been modified to update the state of the compliance semaphore file and to terminate the client's session if the client is admitted to the network and compliance violations are found.

Downloaded from www.Manualslib.com manuals search engine

Note: A number of constraints exist at the time of this writing that affect the processing of the NAC Appliance-specific policy collector. As a result, a number of limitations exist in this version of the collector that can be corrected in a supported version of this collector. In addition, this version of the collector was written quickly in lab conditions and several issues should be corrected in a production version.

Users of this protype version of the policy collector should be aware of the following:

- There is very little error checking, so the collector behaves in unpredictable manners if the configuration is not correct. For example, the policy collector's Handler_Attributes must contain a value called *NACAppliancekickUserCMD* that must contain a command to invoke a Web browser and open a pre-configured HTML form.
- The policy collector is written with JAVA 1.3 and does not have access to the HTTPS classes provided in later JAVA versions. Since an HTTPS Post is required to terminate the client's network session, a special HTML Form has been provided to issue the HTTPS Post request. This form is called by the policy collector and should be customized according to the environment.
- Various attributes required by this special policy collector have been parameterized and can be configured either as parameters of the policy collector or in the Security Compliance Manager Client's handler.properties file.
- All of the components assume that the Security Compliance Manager Client is installed in the c:\Program Files\IBM\SCM\Client directory, which is the default location.

Scheduler

A platform-specific task scheduler (EG Windows Task Scheduler or Cron on UNIX) is configured to run the Security Compliance Manager Client's statuscheck.exe on a periodic basis. This is required to create a *post-admission polling cycle* that monitors the client for compliance after admission to the network. A special scheduler.bat file is provided to create a scheduled task that runs statuscheck.exe each minute. This script is appropriate for Windows clients.

kickrich.html

There are two versions of this HTML form provided, one that requires the user to manually click a button to continue, and one that automatically submits the request. Either one will work and it is up to the reader to decide which behavior is desired. In either case, the selected version should be renamed to kickrich.html if

Downloaded from www.Manualslib.com manuals search engine

using the example HTML form provided. It should be noted that default security settings on most browsers will prevent active content or ask the user whether to allow it, meaning that the user will still have to manually intervene in the process.

This HTML form must be customized to the environment as follows:

- The client's MAC address must be placed in the <INPUT TYPE="HIDDEN" NAME="mac" VALUE="*001125CEF56C*"> tag.
- The administrator UID of the NAC Appliance Manager must be placed in the <INPUT TYPE="HIDDEN" NAME="admin" VALUE="*admin*">
- The password for the specified administrator ID must be placed in the <INPUT TYPE="HIDDEN" NAME="passwd" VALUE="*cisco123*">.

There is sensitive information placed in this file, which is another reason why this version of the integration is not suitable for production.

Installing and configuring prototype integration components

The following instructions are intended to assist the reader in implementing this integration.

NAC Appliance Agent

The prototype version of this agent installs on the client in the same manner as the production version. It is basically a wizard install and there are no configuration parameters required.

On the NAC Appliance Manager, the agent must be registered as follows:

1. Unzip the IBMTivoli.zip file. You will find two sub-directories, CAM and Agent.
2. Copy the two jsps from the CAM sub-directory into the /perfigo/control/tomcat/Webapps/admin/ directory on the Clean Access Manager.
3. Upload the CCAAgentSetup.tar.gz file in the Agent sub-directory on to the Clean Access Manager using **CleanAccess** → **CleanAccess Agent** → **Distribution** with Version 4.0.1.1.

Policy collector

The prototype policy collector is delivered as a .jar file named com.ibm.scm.nac.posture.PolicyCollector.jar. This file is installed as a collector using the Security Compliance Manager Server's Administration Console. This collector is assigned Release Version 500, which is several hundred versions higher than the production versions, to distinguish it from production versions of the collector. Whenever a system with this prototype collector is updated with a production version, the installer will be warned that the new version is lower than

Downloaded from www.Manualslib.com manuals search engine

the old one. This will indicate that the special functionality of this prototype collector will be lost when the production version is installed.

When this collector is included in a compliance policy, it must be configured in the same fashion as a normal policy collector with the following additional requirements:

- The Handler_Attributes parameter must include a value starting with "NACAppliancekickUserCMD=". For example:

  ```
  NACAppliancekickUserCMD="C:\Progra~1\Internet Explorer\iexplore.exe
  C:\Progra~1\IBM\SCM\client\kickrich.html"
  ```

  This example uses default values that will not be valid if software is installed in non-default locations. It is used by the policy collector to start the Internet Explorer browser and load the kickrich.html form provided with the prototype. This in turn informs the Clean Access Manager to place the endpoint in quarantine. If an html form other than the one performed in the example is to be used, this parameter must be changed to use the other form.

- This collector includes a “Network_Enforcement” parameter, which should have the value “cca” added to enable the NAC Appliance integration.

TSCMAgent.bat

This script should be placed in the c:\Program Files\IBM\SCM\Client directory.

NACApplianceCompliance.entry

This file should be placed in the c:\Program Files\IBM\SCM\Client directory.

kickrich.html

This HTML form should be placed in the c:\Program Files\IBM\SCM\Client directory and customized as described in “Integration components” on page 459.

System path

The system path should be modified to include the c:\Program Files\IBM\SCM\Client directory.

Scheduler.bat

This script should be run once on each client system to create a task that calls statuscheck.exe each minute to instantiate post-admission polling. It can be edited before being run to change the frequency of post-admission compliance checks.

Downloaded from www.Manualslib.com manuals search engine

NAC Appliance Manager

A policy on the NAC Appliance Manager must be created to check for the following two requirements:

- The Security Compliance Manager Client is running as a service.
- The c:\Program Files\IBM\SCM\Client\NACApplianceCompliance.properties file exists.

Considerations for designing a production solution

Once the existing prototype components have been integrated in a non-production environment, several facts should become evident that should be considered before designing a production-class solution based on this design. The following is a list of these issues, but it is not to be considered a complete list. Every deployment will have different factors that must be considered, but these items should be common to most deployments.

- Security concerns - Several of the prototype components store sensitive information such as passwords in plain text. This is an advantage for training and discovery but it is also a security vulnerability. Even if the sensitive data is passed to the client in Collector parameters, these are still entered and stored in plain text in the Security Compliance Manager console. In addition, several of the files that are used to capture state on the client are not protected and could be manipulated by users. We recommend that these files be set to hidden, with administrative privileges required to access them.
- Timing - With the current version of the prototype policy collector, there are several possible timing issues that introduce potential vulnerabilities in the solution. Features that are expected in upcoming releases of software should be able to address these vulnerabilities. Most of these are related to post-admission processing.
- Post-admission processing - With post-admission processing, the Security Compliance Manager Client will periodically rescan the endpoint for violations. The normal behavior when a violation is found is to present the remediation handler Interface to the user and proceed as normal. In contrast, the prototype policy collector provided for this integration does not present this interface in this situation. Instead, it marks the endpoint as noncompliant by deleting the compliance semaphore file and then terminates the user's network session, forcing the user to restart the admission process. During this second admission process, the non-existence of the compliance semaphore file will cause the NAC Appliance to quarantine the endpoint, at which point the client will enter the same state as in pre-admission. The prototype version uses the kickrich.html form to initiate the termination of the user's current session, but this situation leaves the user's session active until he responds to the HTML form.

Downloaded from www.Manualslib.com manuals search engine

State mapping and scenarios

One way for the solution to approach a design is to consider all of the possible states that can occur with regards to the client, its compliance state, and its network admission state. Table 8-8 presents the possible states that should be considered.

Table 8-8 Possible client states

State #	Security Compliance Manager Client running	Compliant to policy	Admitted to network
1	0	0	0
2	0	0	1
3	0	1	0
4	0	1	1
5	1	0	0
6	1	0	1
7	1	1	0
8	1	1	1

As indicated by this state table, there are eight different scenarios that must be accommodated in any design. The following list is the expected behavior for each of these states.

- Scenario 1 - Pre-admission, Security Compliance Manager not running, noncompliant client
  - NAC Appliance detects that the Security Compliance Manager Client is not running:
    i. Pops up Temporary Access Window
    ii. User clicks **Update**
    iii. Runs TSCMAgent.bat
  - TSCMAgent.bat:
    i. Sets semaphore to -1
    ii. Starts Security Compliance Manager Client
    iii. Runs statuscheck.exe
  - Statuscheck.exe:
    - Requests rescan from Security Compliance Manager Client

Downloaded from www.Manualslib.com manuals search engine

- Security Compliance Manager Client:
  i. Runs compliance validation. In this case, violations are found and semaphore does not equal 1, so leave semaphore unchanged.
  ii. Since violations are found, client runs remediation handler.
- Remediation handler:
  i. Since semaphore is -1, PopUp Remediation Interface.
  ii. User can click Fix Now for autoremediation.
  iii. Runs compliance validation. In this case, no violations are found, so set semaphore to 1.
- User clicks **Next**.
- NAC Appliance now finds Security Compliance Manager Client running and semaphore=1, so admit client.

- Scenario 2: post-admission, Security Compliance Manager not running, noncompliant client
  - This is a border case and there is no way to address this state.
  - This state can be reached if the user halts the Security Compliance Manager Client after the client has already been admitted to the network and then creates a compliance violation.
  - A potential solution would be a background process that is run by the Windows Scheduler or Cron job to check for the Security Compliance Manager Client to be running and start it if it is not running. This would then bring the client to state #6.
- Scenario 3: pre-admission, Security Compliance Manager not running, compliant client
  - This scenario is a subset of scenario 1.
  - NAC Appliance detects that Security Compliance Manager Client is not running.
    i. Pops up Temporary Access window
    ii. User clicks Update button
    iii. Starts TSCMAgent.bat
  - TSCMAgent.bat:
    i. Sets semaphore to -1
    ii. Starts Security Compliance Manager Client
    iii. Runs statuscheck.exe
  - Statuscheck.exe:
    - Requests posture from Security Compliance Manager Client

Downloaded from www.Manualslib.com manuals search engine

- Security Compliance Manager Client:
  - Runs compliance validation. In this case, no violations are found, so set semaphore to 1.
  - No violations are found so return.
- User clicks Next button.
- NAC Appliance now finds Security Compliance Manager Client running and semaphore=1, so admit client.

- Scenario 4: post-admission, Security Compliance Manager not running, compliant client
  - This is a border case and is similar to scenario 2.
  - This state can be reached if the user halts the Security Compliance Manager Client after the client has already been admitted to the network but the client is actually compliant.
  - A potential solution would be a background process that is run by the Windows Scheduler or Cron job to check whether the Security Compliance Manager Client is running and start it if it is not running. This would then bring the client to state #8.
- Scenario 5 - pre-admission, Security Compliance Manager running, noncompliant client
  - This is the most normal case and is the one that gets demonstrated. It is a subset of scenario 1.
  - NAC Appliance detects that semaphore is not equal to 1.
    i. Pops up Temporary Access window
    ii. User clicks Update button
    iii. Starts TSCMAgent.bat
  - TSCMAgent.bat:
    i. Sets semaphore to -1
    ii. Starts Security Compliance Manager Client (if already running, this step is redundant but not harmful)
    iii. Runs statuscheck.exe
  - Statuscheck.exe:
    - Requests rescan from Security Compliance Manager Client
  - Security Compliance Manager Client
    - Runs compliance scan. In this case, violations are found and semaphore does not equal 1, so leave semaphore unchanged.
    - Since violations are found, run remediation handler

Downloaded from www.Manualslib.com manuals search engine

- Remediation handler:
  - Since semaphore is -1, PopUp Remediation Interface.
  - User can click Fix Now for autoremediation.
  - Runs compliance scan. In this case no violations are found, so set semaphore to 1.
- User clicks Next.
- NAC Appliance now finds Security Compliance Manager Client running and semaphore=1, so admit client.

- Scenario 6 - post-admission, Security Compliance Manager running, noncompliant client
  - In this case, the semaphore starts as 1 since we have been admitted.
  - Windows Scheduler or cron job runs statuscheck.exe.
  - Statuscheck.exe:
    - Requests rescan from Security Compliance Manager Client
  - Security Compliance Manager Client:
    - Runs compliance validation. In this case, violations are found and semaphore equals 1, so set it to 0.
    - Since violations are found, instructs client to run remediation handler.
  - Remediation handler:
    - Since semaphore is 0, call NAC Appliance Kick User API.
    - Exit.
  - NAC Appliance restarts the admission process.
  - Client is now in same state as state #5.

Downloaded from www.Manualslib.com manuals search engine

Since scenarios 5 and 6 are the most complex, the sequence of events for these scenarios is depicted in Figure 8-43.

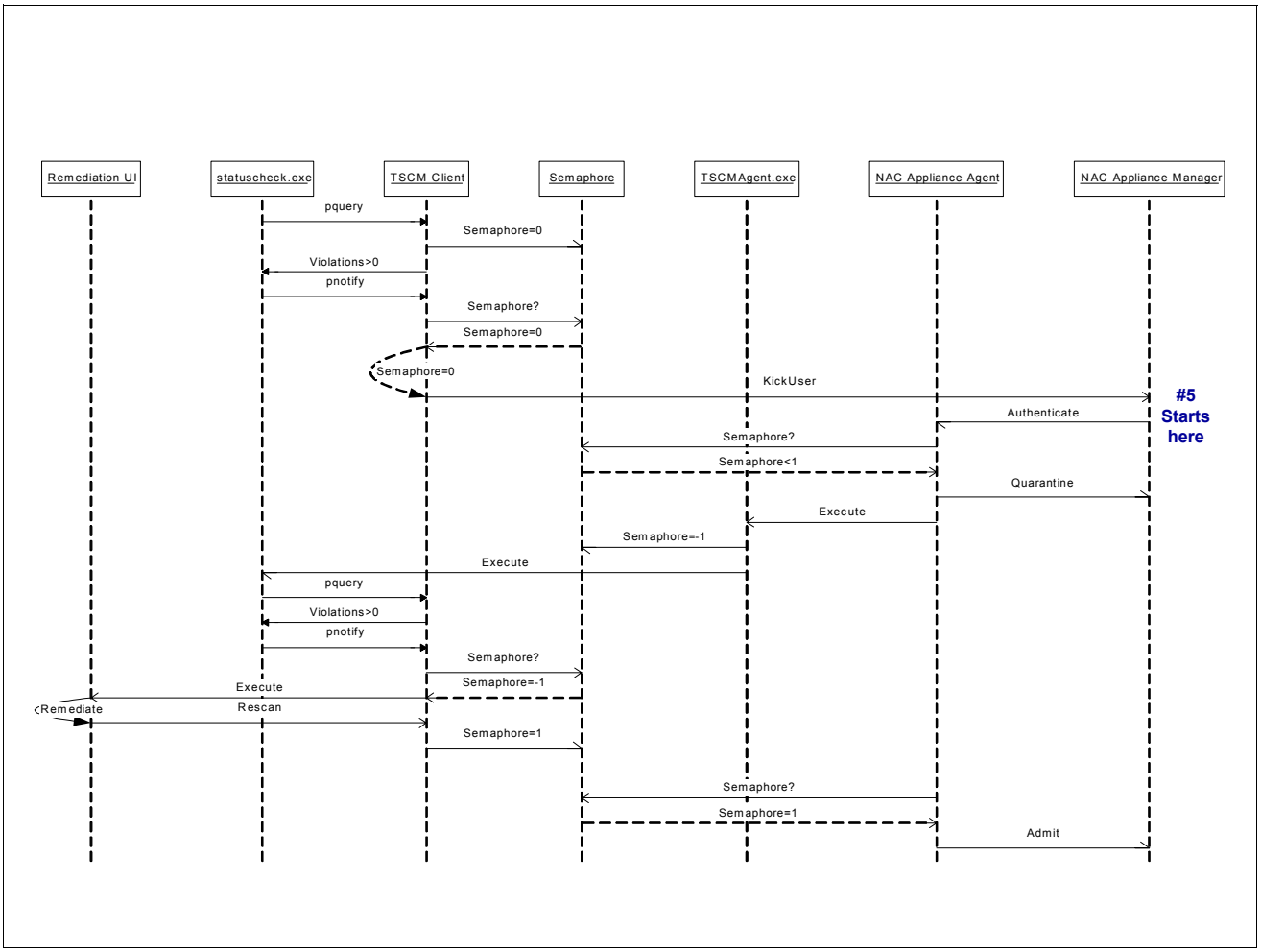


Figure 8-43 Sequence of Events for Scenarios #5 and #6

- Scenario 7 - pre-admission, Security Compliance Manager running, compliant client
  - NAC Appliance restarts admission process.
  - Security Compliance Manager Client is running and semaphore = 1
  - Admit client
- Scenario 8 - post-admission, Security Compliance Manager running, compliant client
  - In this case, the semaphore should start as 1 since we have been admitted.
  - Windows Scheduler or cron job runs statuscheck.exe.

Downloaded from www.Manualslib.com manuals search engine

- Statuscheck.exe:
  - Requests rescan from Security Compliance Manager Client
- Security Compliance Manager Client:
  - Runs compliance validation. In this case, no violations are found.
  - Since violations are not found, exit.

Conclusion

Having read this appendix, you should now have a better understanding of the IBM Integrated Security Solution for Cisco Networks and be familiar with the NAC Appliance offering. The prototype for integration with the NAC Appliance offering should have prepared you to implement this version of the solution in a laboratory or demo environment, and you should now be able to troubleshoot both the NAC Framework and NAC Appliance solutions and their integration with the Tivoli components.

Downloaded from www.Manualslib.com manuals search engine

B

Network Admission Control

In this appendix we discuss the Network Admission Control initiative from Cisco Systems. This appendix contains a Cisco white paper that is publicly available at the following address:

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd800fdd66.shtml

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Executive summary

Emerging network security threats, such as viruses, worms, and spyware, continue to plague customers and drain organizations of money, productivity, and opportunity. Meanwhile, the pervasiveness of mobile computing has increased this threat. Mobile users are able to connect to the Internet or the office from home or public hotspots — and can easily and often unknowingly pick up a virus and carry it into the corporate environment, thereby infecting the network.

Network Admission Control (NAC) has been designed specifically to ensure that all endpoint devices (such as PCs, mobile computers, servers, smartphones, and PDAs) accessing network resources are adequately protected from network security threats. NAC's market-leading solutions, which have been embraced by leading antivirus, security, and management manufacturers, have captured the attention of the press and analyst communities, as well as organizations of all sizes.

This appendix explains the vital role that NAC can play as part of a policy-based security strategy, and describes and defines the available NAC approaches.

The benefit of NAC

Despite years of security technology development and millions of dollars spent in implementation, viruses, worms, spyware, and other forms of malware remain the primary issue facing organizations today, according to the 2005 CSI/FBI Security Report. The large numbers of incidents organizations face annually result in significant financial impact due to downtime, lost revenue, damaged or destroyed data, and loss of productivity.

The message is clear: traditional security solutions alone have not been able to address this problem. In response, Cisco Systems has developed a comprehensive security solution that brings together leading antivirus, security, and management solutions to ensure that all devices in a networked environment comply with security policy. NAC allows you to analyze and control all devices coming into your network. By ensuring that every endpoint device complies with corporate security policy (that they are running the latest and most relevant security protections, for example), organizations can significantly reduce or eliminate endpoint devices as a common source of infection or network compromise.

Downloaded from www.Manualslib.com manuals search engine

Dramatically improve network security

While most organizations use identity management and authentication, authorization, and accounting (AAA) to authenticate users and authorize network privileges, there has been virtually no way to authenticate the security profile of a user's endpoint device. Without an accurate way to assess the health of a device, even the most trustworthy user can inadvertently expose everyone else in the network to significant risks posed by either an infected device or by one that is not properly protected against infection.

NAC is a set of technologies and solutions built on an industry initiative led by Cisco Systems. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers implementing NAC are able to restrict network access to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can control the access of noncompliant or unmanaged devices.

NAC is unique because it is designed to be integrated into the network infrastructure. So why should a policy compliance and verification strategy be implemented in the network instead of somewhere else?

- Virtually every bit of data that an organization is interested in or is concerned about touches the network.
- Virtually any device that an organization is interested in or concerned about is attached to that same network.
- Implementing admission control in the network gives an organization the ability to deploy the broadest possible security solution covering the largest number of networked devices.
- This strategy uses an organization's existing infrastructure, security, and management deployments, so it has the smallest IT overhead footprint possible.

With NAC in place, whenever an endpoint device attempts to make a network connection, the network access device (LAN, WAN, wireless, or remote access) automatically requests a security profile of the endpoint device, which is provided either through an installed client or through assessment tools. This profiled information is then compared to network security policy, and the level of device compliance to that policy determines how the network handles the request for admission. The network can simply permit or deny access, or it can restrict access by redirecting the device to a network segment that limits exposure to potential vulnerabilities. It can also quarantine a noncompliant device by redirecting it to a remediation server, where it may be updated with components that will bring it into policy compliance.

Downloaded from www.Manualslib.com manuals search engine

Some of the security policy compliance checks that NAC can perform include:

- Determining whether the device is running an authorized version of an operating system.
- Checking to see if the OS has been properly patched or has received the latest hotfix.
- Determining whether the device has antivirus software installed, and whether it has the latest set of signature files.
- Ensuring that antivirus technology is enabled and has been run recently.
- Determining whether personal firewall, intrusion prevention, or other desktop security software is installed and properly configured.
- Checking whether a corporate image of a device has been modified or tampered with.

Answers to these and similar security profile questions are then used to make intelligent, policy-based decisions regarding network admission.

Some of the benefits of implementing a NAC solution include:

1. Dramatically improved security of any network, regardless of size or complexity, by helping to ensure that all user network devices conform to security policy. By proactively protecting against worms, viruses, spyware, and malware, organizations are able to focus operations on prevention, rather than on reaction.
2. Extended value of existing investments in the Cisco network, as well as in antivirus, security, and management software, through broad adoption and integration by leading manufacturers.
3. Increased enterprise resilience and scalability by providing a means to inspect and control all devices that connect to the network, regardless of their access methods (routers, switches, wireless, VPN, dialup, for example).
4. Preventing noncompliant and unmanaged endpoint devices from affecting network availability or user productivity.
5. Reduced operating expenses related to identifying and repairing noncompliant, unmanaged, and infected systems.

NAC implementation options

Cisco offers both appliance-based and architecture-based framework approaches to NAC that meet the functional and operational needs of any organization, whether they have a simple security policy requirement or require

Downloaded from www.Manualslib.com manuals search engine

support for a complex security implementation involving a number of security vendors, combined with a corporate desktop management solution.

The NAC Appliance, available as Cisco Clean Access, provides rapid deployment with self-contained endpoint assessment, policy management, and remediation services. In addition, the NAC Framework integrates an intelligent network infrastructure with solutions from more than 50 manufacturers of leading antivirus and other security and management software solutions.

The NAC Appliance

The NAC Appliance products, delivered through the Cisco Clean Access product line, provide rapid deployment with self-contained endpoint assessment, policy management, and remediation services. This rapidly deployable *solution-in-a-box* technology automatically detects, isolates, and cleans infected or vulnerable wired or wireless endpoints attempting to access a network.

Cisco Clean Access provides three critical protection functions:

- Recognizes users, their devices, and their roles in the network, at the point of authentication authorization
- Evaluates the security posture of endpoints using either scanning and analysis technology or a lightweight agent for deeper posture assessment, to check for vulnerabilities
- Enforces security policy in the network by blocking, quarantining, and repairing noncompliant endpoints

Cisco Clean Access also provides the following implementation benefits:

- Scalability - Cisco Clean Access can be deployed immediately to address network admission needs while designing and evaluating the NAC Framework, since Cisco Clean Access components can be integrated into the broader NAC Framework architecture.
- Rapid deployment - Cisco Clean Access is a *shrink-wrapped*, out-of-the-box solution with pre-installed support for antivirus, antispyware, and Microsoft updates.
- Flexibility - Cisco Clean Access supports a heterogeneous network infrastructure with multiple desktop operating systems.

Network characteristics that are ideal for selecting Cisco Clean Access include:

- A non-802.1x LAN environment
- Wireless, branch, remote, or simple LAN environments
- Centralized IT environment and management

Downloaded from www.Manualslib.com manuals search engine

- Network access by unmanaged computers (such as guests, contractors, or students)
- A heterogeneous (multivendor) network infrastructure

NAC Framework solution

NAC is also available as an architecture-based framework solution that is designed to leverage an existing base of both Cisco network technologies and existing deployments of security and management solutions from other manufacturers.

A NAC Framework solution provides the following benefits:

- Comprehensive span of control by assessing all endpoints across all access methods, including LAN, wireless, remote access, and WAN
- Endpoint visibility and control to help ensure that managed, unmanaged, guest, and rogue devices meet corporate security policies
- Life-cycle support for endpoint control that automates the assessment, authentication, authorization, and remediation of endpoints
- A combination of central policy management, intelligent network devices, and network services with solutions from dozens of leading antivirus, security, and management vendors, to provide granular admission control management
- Support for a rich ecosystem of partners and technologies through standards-based, flexible APIs that allow multiple third parties to contribute to the overall solution

The following network characteristics are optimal for a NAC Framework deployment:

- Large-scale enterprise deployments
- A sophisticated LAN/WAN/wireless environment
- A LAN/WAN/wireless infrastructure that is entirely or primarily based on Cisco technology
- Operational interoperability with NAC partner security and management solutions
- IP telephony implementations or planned implementations
- 802.1X implementations or planned implementations

Investment protection

Cisco offers the most comprehensive set of admission control products and solutions to meet the functional needs of any organization. And because many

Downloaded from www.Manualslib.com manuals search engine

organizations have evolving needs, Cisco Clean Access product components that are installed now can be used to support a later NAC Framework implementation.

Regardless of which approach you decide is appropriate for your environment, Cisco NAC technologies are designed to preserve your investments in corresponding network technology. At the same time, interoperability and functional compatibility help ensure a smooth transition from Cisco Clean Access to the additional benefits and capabilities of the NAC Framework technology.

Planning, designing, and deploying an effective NAC solution

To help ensure that your Cisco NAC deployment is a success, Cisco Advanced Services offers the following requirements analysis, planning, design, and implementation services:

- NAC Readiness Assessment

  Analyzes deployment requirements and assesses the readiness of your network devices, operations, and architecture to support NAC

- NAC Limited Deployment

  Provides installation and configuration of a limited deployment solution, allowing your staff to test and gain experience with NAC

- NAC Design Development

  Assists your team in developing a detailed design for integrating NAC into your network infrastructure

- NAC Implementation Engineering

  Supports your team through a full-scale implementation by developing detailed plans installation, configuration, integration, and management plans and providing on-site installation, configuration, and testing to help ensure that the deployment integrates smoothly into your production environment

Once NAC is deployed, Cisco Technical Support Services are available to complement your internal resources and help ensure that Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

Downloaded from www.Manualslib.com manuals search engine

The next steps

Let us take a look at the next steps:

1. Deploy Cisco Clean Access now. Cisco Clean Access allows you to immediately receive the benefits of an admission control solution.
2. Determine whether you will need an architecture-based NAC Framework solution. With Cisco Clean Access in place, you can begin to evaluate whether you also meet a profile for an architecture-based approach. Several factors must be considered when choosing to deploy any NAC solution, including the network where it is to be deployed and the type of organization that is deploying it.
3. Consider getting help. Cisco Advanced Services can assist you with the design, implementation, integration, and deployment of a customized NAC solution.
4. Take advantage of your Cisco Clean Access investment. Cisco Clean Access components can be fully integrated into a NAC Framework solution.

NAC technology

Let us take a look at the components needed for NAC Appliance and NAC Framework.

NAC Appliance components

Cisco Clean Access is comprised of the following elements:

- Cisco Clean Access Server provides device assessment and enforces access privileges based on endpoint compliance.
- Cisco Clean Access Manager provides central management of the Cisco Clean Access solution, including enforcement policy and remediation services.
- Cisco Clean Access Agent is an optional, free client that provides more rigorous endpoint policy compliance assessment and streamlined remediation in both managed and unmanaged environments.

Cisco Clean Access is supported for wireless access via the following technologies:

- All 802.11 Wi-Fi access points, including Cisco Aironet access points
- Any Wi-Fi client devices with an IEEE 802.1X supplicant that supports NAC

Downloaded from www.Manualslib.com manuals search engine

NAC Framework components

The NAC Framework provides the following technology support:

- Broad network device support for campus LANs, WANs, VPNs, and wireless access points
- Ties to third-party host assessment tools for unmanned, *agentless*, and other nonresponsive devices, and is able to apply a different policy to each device
- Broad platform support for the Cisco Trust Agent
- Extends multivendor integration, with application and operating system status checks that go far beyond antivirus and basic operating system patches

The NAC Framework is supported by the following technologies:

- Cisco routers:
  - Cisco 83x, 18xx, 28xx, and 38xx series integrated services routers
  - 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760 modular access routers
  - 2600XM, 2691, 3640, and 3660-ENT multiservice access routers
  - 72xx Series routers
- Cisco switches:
  - Cisco Catalyst 6500 Series Supervisor Engine 2, 32, and 720, with Cisco Catalyst OS, Cisco IOS Software, or hybrid applications (Cisco IOS Software support on Supervisor Engine 32 and 720)
  - Cisco Catalyst 4000 Series Supervisor Engine II+, II+TS, IV, V, and V-10GE, with Cisco IOS Software
  - Cisco Catalyst 4948 and 4948-10GE
  - Cisco Catalyst 3550, 3560, and 3750, with Cisco IOS IP base and IP services
  - Cisco Catalyst 2940, 2950, 2955, 2960, 2970
- Cisco wireless access: Cisco Aironet access points, Cisco Aironet lightweight access points connected to a Cisco Wireless LAN Controller, the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), and all Cisco Aironet, Cisco Compatible, and Wi-Fi client devices with an IEEE 802.1X supplicant that supports NAC
- Cisco VPN 3000 Series concentrators
- Cisco Trust Agent
- Cisco Secure Access Control Server (ACS)
- Third-party vendor software

Downloaded from www.Manualslib.com manuals search engine

- Recommended components:
  - Cisco Security Agent
  - Cisco Security Monitoring, Analysis, and Response System (MARS)
  - CiscoWorks Security and Information Management Solution (SIMS)

For more information visit:

http://www.cisco.com/go/nac

Downloaded from www.Manualslib.com manuals search engine

C

Additional material

This redbook refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this redbook is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

`ftp://www.redbooks.ibm.com/redbooks/SG246678`

Alternatively, you can go to the IBM Redbooks Web site at:

`ibm.com/redbooks`

Select the **Additional materials** and open the directory that corresponds with the redbook form number, SG246678.

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Using the Web material

The additional Web material that accompanies this redbook includes the following files:

File name	*Description*
IBM Tivoli - CCA Agent.zip	Contains the Cisco Clean Access Agent Version 4.0.1.1 used for our example
NACAppliancePrototype.zip	Contains the necessary files (policy collector, remediation html files, and so on) that have been used in our sample scenario

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

Downloaded from www.Manualslib.com manuals search engine

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 484. Note that some of the documents referenced here may be available in softcopy only.

- *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450
- *Deployment Guide Series: IBM Tivoli Configuration Manager*, SG24-6454
- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Security Compliance Manager Version 5.1: Administration Guide*, SC32-1594
- *IBM Tivoli Security Compliance Manager Version 5.1: Installation Guide: All Components*, GC32-1592
- *IBM Tivoli Security Compliance Manager Version 5.1: Installation Guide: Client Components*, GC32-1593
- *IBM Tivoli Configuration Manager Release Notes (Revised June 2006) Version 4.2.3*, GI11-0926-05
- *IBM Tivoli Configuration Manager Planning and Installation Guide Version 4.2.3*, GC23-4702-03
- *IBM Tivoli Configuration Manager User's Guide for Software Distribution Version 4.2.3*, SC23-4711-03
- *IBM Tivoli Configuration Manager User's Guide for Deployment Services Version 4.2.3*, SC23-4710-03

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

Online resources

These Web sites and URLs are also relevant as further information sources:

- Gramm-Leach-Bliley Act (GLBA)

  http://banking.senate.gov/conf/

- Sarbanes-Oxley Act (SOX)

  http://www.sarbanes-oxley.com

- Health Insurance Portability and Accountability Act (HIPAA)

  http://www.cms.hhs.gov/hipaa

- Cisco Secure Access Control Server

  http://www.cisco.com/go/acs

- Cisco Network Admission Control

  http://www.cisco.com/go/nac

- Cisco Trust Agent documentation

  http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cta/cta1_0/index.htm

- IBM Tivoli Security Compliance Manager Installation Guide

  http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp?topic=/com.ibm.itscm.doc_5.1/scm51_install.html

- IBM Tivoli Configuration Manager online documentation

  http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.tivoli.itcm.doc/toc.xml

- IBM Tivoli Security Compliance Manager 5.1 Utilities

  http://www.ibm.com/support/docview.wss?rs=2004&context=SSVHZU&dc=D400&q1=utilities&uid=swg24007082&loc=en_US&cs=utf-8&lang=en

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications, and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

http://www.redbooks.ibm.com

Downloaded from www.Manualslib.com manuals search engine

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Index

Numerics

802.1x 16, 22, 26, 68, 81, 95, 265
  credentials 112

A

access control list 34
  configuration 293
  dynamic 216
Access Control Server 18, 23, 25, 36, 41, 54, 101
  action parameter 58
  administrative interface 216
  authorization rule configuration 280
  certificate setup 219
  clientless user 283
  configuration for NAC L2 802.1x 214
  configuration for NAC L2/L3 IP 283
  csutil.exe 225
  CTA certificate 191
  downloadable ACL 284
  external user database 283
  group configuration 237
  high availability 36
  HTTP administrator access 218
  logging 60, 223, 226, 302
  Network Access Filter 287
  physical components 118
  policy 99, 109
  policy creation 58
  PolicyVersion 442
  Security Compliance Manager attributes 223
  self-signed certificate 220
  system posture token 114
  troubleshooting 453
  unknown user policy 283
  violation count 442
Access Manager for e-business 85
access policy 58, 60
action parameter 58
administrators
  involvement 26
admission control client 43
antivirus collector configuration 163
application posture token 59
architecture
  overview 14
audit
  readiness 85
authentication 41
  configuration for ACS 241
authorization rule configuration 280
automated remediation 4, 21, 27, 444
  prerequisites 358
  remediation client configuration 357
autonomic computing 4
availability 30
avoid business disruptions 398

B

bandwidth restriction 327
Base64-encoded X.509 219
benefits 9
build phase 35
business disruptions
  avoiding ... 398
business requirements 95

C

certificate 191
  revocation list 219
  trust list 219
checkup 59
  system posture token 114
Cisco
  Catalyst 3750 291
  IOS router 291
  Secure Access Control Server
    see Access Control Server
  Security Agent 53
  self-defending network 16
Cisco Trust Agent 18, 23, 53, 101
  dot1x supplicant 190
  encapsulated authentication protocol 45
  EXT-Posture plug-in 44
  installation 89, 190
  Logging Service 44
  PEAP session 191

© Copyright IBM Corp. 2005, 2007. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

physical components 121
pop-up notification 277
posture plug-in 44, 51
posture status reply 59
SCM client communication 48
secure communication 63
Service 44
troubleshooting 453
violation count 58
Clean Access Agent 45, 82, 456, 478
configuration 303, 334
Clean Access Manager 45, 82, 303, 455, 478
policy 99
Clean Access Server 18, 45, 82, 303, 455, 478
compliance check 99
client network access 59
clientless hosts
configuration 300
clientless user 283
collector 18, 49, 442
antivirus configuration 163
hotfixes 169
password settings 165
personal firewall 171
posture collector 153
service pack level 167
service running 177
com.ibm.scm.nac.posture.PolicyCollector 357
com.ibm.scm.nac.tcmremed.client.TCMRemed 357
communication
flow 55
security 62
comparison
between NAC Framework and NAC Appliance 17
compliance 85
check 99
component implementation 125
concept 4
criteria 103
criteria for workstations 100
data 18
decisions 103
exception 29
management
business process 28
policy 57, 395
assigning to clients 186
configuration 152
customization 161
versioning 103
posture collector 153
query 19
report 46
requirements 96
server 34
status for workstations 97
status reports 29–30
user interface 20
violation 50
confidentiality 30
configuration
Access Control Server
authentication and authorization 241
authorization rule 280
certificate setup 219
downloadable ACL 284
for NAC L2 802.1x 214
for NAC L2/L3 IP 283
groups 237
logging 226
posture validation 244
ACLs 293
administrative interface to Access Control Server 216
antivirus collector 163
Clean Access Agent 303, 334
clientless hosts 300
compliance policy 152
hotfix collector 169
HTTP administrator access for ACS 218
NAC Appliance components 303
NAC Framework 214
network access profile 271, 289
network interface 301
out-of-band virtual gateway 306
password settings collector 165
personal firewall collector 171
policy collector 358
posture validation process 299
RADIUS Authorization Components 264, 287
RADIUS for NAC 236
remediation
client 357
packages 417
server 385
workflows 417

Downloaded from www.Manualslib.com manuals search engine

service pack level collector 167
service running collector 177
Software Package Utilities 394
Software Package Web Server 386
switch configuration for NAC Appliance 352
Tivoli Configuration Manager 358
Tivoli Configuration Manager Web Gateway 359
configuration change process 32
controlled network zone 66
corporate
compliance 3
security policy 8
csutil.exe 225
ctaCert.exe 198

D

data flow 55
day zero attacks 53
DB2 Alphablox 17
default
access policy 59
login page 315
remediation handler 51
definition phase 35
deployment
overview 442
scenarios 65
DER-encoded binary X.509 219
design phase 35
dialup 16
NAC enablement 27
dot1x reauthentication timer 270
dot1x supplicant 190
downloadable ACL 284
dynamic access control list 216

E

EAP 45
see Extensible Authentication Protocol
EAPoRADIUS 59
EAPoUDP 59
AAA configuration 299
NAC L2/L3 IP 284
EAPoverLAN 16
EAPoverUDP 16
emergency change procedure 95, 97
encapsulated authentication protocol 45
endpoint posture credentials 43
enduser challenges 97
error handling 448
Extensible Authentication Protocol 16, 23
session initiation 59
EXT-posture plug-in 44

F

failing rule 174
fault isolation 448
Financial Services Modernization Act 6
flow of communication 55
functional requirements 96

G

GLBA 6
grace period 398
Gramm-Leach-Bliley Act 6
guest VLAN 114, 283

H

health check 28
Health Insurance Portability and Accountability Act 6
healthy 59
system posture token 114
high availability 35
HIPAA 6
Host IDS 53
Hot Standby Routing Protocol 36
hotfix 40, 95, 97
collector configuration 169
HTML
debugging attributes 406
remediation example pages 409
remediation information 116, 398

I

IBM Method for Architecting Secure Solution 63
IBM Method for Architecting Secure Solutions 14
IBM Solution Assurance Review Process 88
IBM Tivoli Access Manager for e-business
see Access Manager for e-business
IBM Tivoli Configuration Manager
see Tivoli Configuration Manager
IBM Tivoli Identity Manager
see Identity Manager

Downloaded from www.Manualslib.com manuals search engine

IBM Tivoli Security Compliance Manager
see Security Compliance Manager
identity
... based networking services 95
Identity Manager
Access Control Server provisioning 25
IEEE 802.1x 16, 22, 26, 68, 81, 95, 265
credentials 112
in-band 45
... vs. out-of-band 456
NAC Appliance deployment 303
infected 60
system posture token 114
initiation phase 35
installation
... of Cisco Trust Agent 190
integrity 30
Internet
access proxy 34
IOS router
useful commands 452
IP telephony devices 300
IP-connected printers 300
IPSec 16

L

Layer 2 NAC 16, 22, 33, 112
Layer 3 NAC 16, 21, 33
logging
Access Control Server 226, 302
posture policy HTML 406
service 44

M

machine authentication 112
manual remediation 116
MASS 14, 63
matching rule 174
Method for Architecting Secure Solutions 14, 63
mobile user 96
monitoring 226

N

NAC
see network admission control
NAC Appliance 17, 45, 82, 475
Clean Access Agent configuration 334
comparing with NAC Framework 17
components 455
configuration 303
default login page 315
port profile 320
SNMP receiver 323
switch configuration 352
switch group 316
switch profile 319
traffic policy 329
user roles 327
NAC Framework 80, 476
comparing with NAC Appliance 17
configuration 214
NAC L2 802.1x
switch configuration 291
NAC L2 IP
switch configuration 291, 295
NAC L3 IP
router configuration 291, 298
NAD
see network access device
network
access control
requirements 96
access decision 99
access filtering 217, 287
access profile 112, 271, 289
administrators involvement 26
admission
check 106
policy 103
bandwidth 35
design factors 33
device group 112, 229
enforcement subsystem 213
identity provisioning 24
infrastructure 26
deployment 291
interface configuration 301
performance 34
perimeter security 80
policy enforcement 60
protocol layer 2 33
security 63, 96, 473
step-up security 24
zone 64
network access device 35–36, 43, 54, 101
configuration 58

Downloaded from www.Manualslib.com manuals search engine

configuration in ACS 229
network policy enforcement 60
placement 67
polling of posture status 61
posture validation 59
PostureQuery 444
session initiation 59
network admission control 15, 78, 87
appliance 17, 45
authentication server 214
clientless user 283
deployment scenario 27
external user database 283
guest VLAN 283
identity based decision 22
implementation phase 88
overview 471
performance controls 34
physical components 118
posture based decision 21
process 20, 444
revalidation period 34
sequence of events 447
status query period 34
networking
identity based services 95
non-responsive hosts
configuration 300

O

object 25, 57
operational cost 98
out-of-band 45, 82
... vs. in-band 456
NAC Appliance deployment 303
virtual gateway configuration 306

P

password
quality standards 95
settings collector configuration 165
PEAP 59
client session 60
PEAP session 191
performance controls 34
personal firewall 53
collector configuration 171
physical components 52
pnotify 454
Point-to-Point Protocol 23
policy 8
collector 50, 53, 57, 61, 104, 153–154, 357, 444
configuration 358
compliance solution 46
creation 26, 58
... and deployment 56
deployment 57
enforcement 32
device 43
implementation 31
life cycle management 30
violation 20
PolicyVersion 442, 444
polling the client 43
pop-up notification 277
port profile 320
posture
agent 24, 34
cache 50, 58, 454
cache data
age 106
conceptual flow 107
check status 357
client request 99
collection process 58
collector 18, 48, 50, 53, 57–58, 103, 153, 395
workflow attributes 403
credentials 43–44, 50
criteria 58
data collection 50
element HTML 402
item HTML 400
plug-in 44, 48, 51, 199, 212
policy 89
HTML debugging attributes 406
version 104, 110
query 59
status 20, 154
determination 50
information 110
reply 59
token 444
validation 54, 59
configuration 244
policy 112
process enablement 299
server 32, 41, 43, 50

Downloaded from www.Manualslib.com manuals search engine

timers 301
PostureNotification 447
PostureQuery 444, 447
PPP
see Point-to-Point Protocol
pquery 454
printer
IP-connected 300
process 444
productivity
loss of ... 95
project
plan 88
scope 27
Protected Extensible Authentication Protocol 59
protocol type 112
provisioning 19
Provisioning Manager 36
object 57
remediation artifacts 442
pstatuschange 454
pull mode 206
push mode 206

Q

quarantine 20, 32, 34, 60–61, 99
access 33
system posture token 114

R

RAC
see RADIUS Authorization Component
RADIUS 16, 23, 42, 54
attributes 112
Authorization Component configuration 264
Authorization Components 112
configuration 287
configuration for NAC 236
response 60
Redbooks Web site 484
Contact us xiii
registry values 174
remediation 4, 27, 444
artifacts 442
client configuration 357
concept 4
configuration for manual ... 116
handler 20, 25, 50, 52, 61, 100–101, 357, 454
request URL 108
HTML example 409
HTML information 398
instructions for the users 397
JAVA classes 108
listener 90
methodology 100
network 20, 32, 99
network access 99
object 19, 25, 57
package
configuration 417
location 252
prerequisites 358
process 8, 25, 29, 61
defining manual remediation 91
definition 26
request URL 108
requirement 97
server 25, 34, 51
configuration 385
service 100
servlet 52
TCRMessengerDisabled workflow 435
TCRMSPatchesInstallWinXP workflow 426
TCRMSServicePackInstallWinXpSp2 workflow 429
TCRNavScan workflow 418
TCRNavSoftwareInstalled workflow 425
TCRNavVirusDefUpdate workflow 423
TCRZLSoftwareInstalled workflow 432
TCRZLSoftwareRunning workflow 434
URL 60
workflow 19, 91, 394
configuration 417
reporting 226
compliance 46
restricted network zone 66
revalidation period 34
risk
acceptance 29
assessment 30
root certificate 191
router
compliance check 99
high availability 36
useful commands 452
rule 174

Downloaded from www.Manualslib.com manuals search engine

S

Sarbanes-Oxley Act 6
scalability 35, 357
scope of the project 27
Secure Access Control Server
    see Access Control Server
secure communication 62
secure PEAP session 191
security
    compliance
        concept 4
        criteria 100
        data 18, 46
        exception 29
        management
            business process 28
    officers involvement 26
    policy 8, 19, 28
        enforcement 32
        implementation 31
        lifecycle management 30
    posture credentials 41
    zone 64
Security Compliance Manager 17, 36, 46, 78, 102
    administration 47
    attributes for ACS 223
    client 48, 53, 104
        installation 89, 189, 199
        troubleshooting 454
    collector 18, 49, 442
    communication 450
        ports 145
    compliance
        evaluation 48
        policy 57
        query 19
        reporting 47
    data collection 47
    implementation phase 88
    operational costs 98
    physical components 117
    policy 53
        collector 50, 444
        deployment 57
        violation 20
    PolicyVersion 444
    posture collector 18, 50, 153
    posture credentials 50
    posture policy 89
    posture status 20
    push/pull mode 206
    remediation handler 50
    rule 174
    secure communication 63
    security certificate 146
    security compliance data 18
    security policy 19
    server 46, 54
        setup 126
    snapshot 20
    software versions 118
    TCMCLI policy 189
    violation count 50, 444
self-defending network 4, 16
self-signed certificate 191, 220
service pack level collector configuration 167
service running collector 177
session duration 327
snapshot 20
SNMP receiver 323
software distribution
    depot 34
    server 102
Software Package Block 417
Software Package Utilities 394
Software Package Web server 357, 386
solution flow 55
SOX 6
sputil.sh 417
Statement of Work 35
status query period 34
StatusChangeQuery 447
stepped-up network security 24
supplicant 23
switch 33
    compliance check 99
    configuration for NAC Appliance 352
    group 316
    profile 319
switched virtual interface 114
switching 16
system integrator 44
system posture token 59, 114

T

TACACS+ 36, 42
TCMCLI policy 189

Downloaded from www.Manualslib.com manuals search engine

TCRMessengerDisabled workflow 435
TCRMSPatchesInstallWinXP workflow 426
TCRMSServicePackInstallWinXpSp2 workflow 429
TCRNavScan workflow 418
TCRNavSoftwareInstalled workflow 425
TCRNavVirusDefUpdate workflow 423
TCRZLSoftwareInstalled workflow 432
TCRZLSoftwareRunning workflow 434
telephony
  IP based devices 300
third party posture plug-in 44
threat identification 30
timer for posture validation 301
Tivoli Configuration Manager 7, 19, 51, 55, 61, 78, 102, 355
  configuration 358
  operational costs 98
  physical components 122
  remediation handler 357
  remediation workflow 19
  secure communication 63
  Software Package Block 417
  Software Package Utilities 394
  Software Package Web Server 386
  Software Package Web server 357
  TCMCLI policy 189
  Web Gateway configuration 359
  Web Gateway installation 375
  Web Gateway user account 375
Tivoli Framework 51
totel cost of ownership 27
traffic policy 327, 329
transition system posture token 114
troubleshooting 226, 448
trusted network 34

U

UDP
  see User Datagram Protocol
unauthorized
  Windows services 95
uncontrolled network zone 65
unknown 60
  system posture token 114
  user policy 283
URL
  for remediation 60
URL-redirection 300, 302
user authentication 112
User Datagram Protocol 23
user roles 327

V

validation
  criteria 41
violation
  count 50, 58, 110, 114, 442, 444
  description 101
virtual LAN 33
virtual private network
  see VPN
VLAN 33
  assignment 327
  dynamical placements of users 237
  membership 83
VPN 7, 65
  concentrator 33
  NAC enablement 27
vulnerability 8

W

Windows services
  unauthorized 95
wireless access 16
wireless access point 33
work-at-home user 96
workflow attribute 403
workstation
  compliance status 97

Downloaded from www.Manualslib.com manuals search engine

Redbooks

Building a Network Access Control Solution with IBM Tivoli and Cisco Systems

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Building a Network Access Control Solution

with IBM Tivoli and Cisco Systems

Redbooks

Covering Cisco Network Admission Control Framework and Appliance

Automated remediation of noncompliant workstations

Advanced security compliance notification

The increasing number of endpoints used to access a network in any enterprise environment can greatly affect security. Endpoints that connect to the enterprise and are corrupted in some way can infect other parts of the enterprise and cause significant IT infrastructure damage and loss of productivity. Additionally, organizations must address security compliance as they are faced with an increasing numbers of internal, industry, and government policies, standards, and regulations.

This IBM Redbook discusses the IBM Integrated Security Solution for Cisco Networks, which offers a security-rich, policy-based security compliance and remediation solution for small, medium, and large businesses. We explain how administrative tasks can be simplified by centralizing the administration of defined security policies, automating security policy enforcement and execution, and automating endpoint security scans. As a result we can create notifications of security compliance vulnerabilities, quarantine, and automatically remediate noncompliant workstations before a potential security incident occurs.

This book is targeted at security professionals, architects, and senior security and IT managers to provide valuable architectural, technical, and planning information.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6678-01 ISBN 0738489883

Downloaded from www.Manualslib.com manuals search engine